

E6303-01

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-149417

(43)Date of publication of application : 30.05.2000

(51)Int.Cl.

G11B 20/10
G06F 3/06
G06F 12/14
H04H 1/00
H04L 9/08
H04L 9/32

(21)Application number : 10-312596

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 02.11.1998

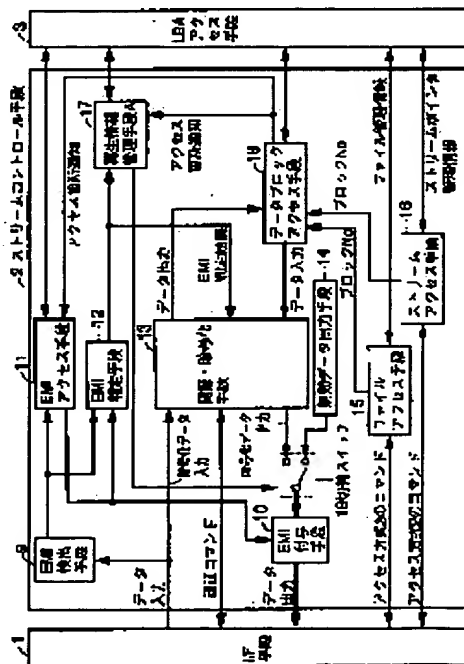
(72)Inventor : KUNO YOSHIKI
NISHIMURA TAKUYA
TAKECHI HIDEAKI
YAMADA MASAZUMI
IIZUKA HIROYUKI
GOTO SHOICHI

(54) RECORDING AND REPRODUCING DEVICE, PROGRAM RECORDING MEDIUM, AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a recording and reproducing device and a program recording medium therefor capable of transferring AV data from a once-recorded recording medium to another recording medium when utilization duplication is permitted only once by program utilization license information.

SOLUTION: This recording and reproducing device is provided with a recording means 11, 17, 18, and a reproducing means 11, 17, 18, 19 for reproducing only once an AV data recorded by the recording means 11, 17, 18 when signal information showing AV data utilization permission information represents a duplication inhibit permitting viewing and listening only one. An EMI judging means 12 judges the presence or absence and the kind of the utilization permission from the EMI information. An authenticating and enciphering means 13 performs authentication between AV apparatuses via a digital I/F means 1, and deciphers the AV data inputted from the I/F means 1, and also enciphers the AV data read from a disk medium 6 side via a data block accessing means 18.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than
the examiner's decision of rejection or
application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-149417

(P2000-149417A)

(43)公開日 平成12年5月30日 (2000.5.30)

| (51)Int.Cl. | 識別記号 | F I | テマコード(参考) |
|---------------|-------|---------------|-------------------|
| G 1 1 B 20/10 | | G 1 1 B 20/10 | H 5 B 0 1 7 |
| G 0 6 F 3/06 | 3 0 1 | G 0 6 F 3/06 | 3 0 1 A 5 B 0 6 5 |
| 12/14 | 3 2 0 | 12/14 | 3 2 0 F 5 D 0 4 4 |
| H 0 4 H 1/00 | | H 0 4 H 1/00 | F 5 J 1 0 4 |
| H 0 4 L 9/08 | | H 0 4 L 9/00 | 6 0 1 B |

審査請求 未請求 請求項の数23 OL (全 32 頁) 最終頁に続く

(21)出願番号 特願平10-312596

(22)出願日 平成10年11月2日 (1998.11.2)

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 久野 良樹

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 西村 拓也

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74)代理人 100092794

弁理士 松田 正道

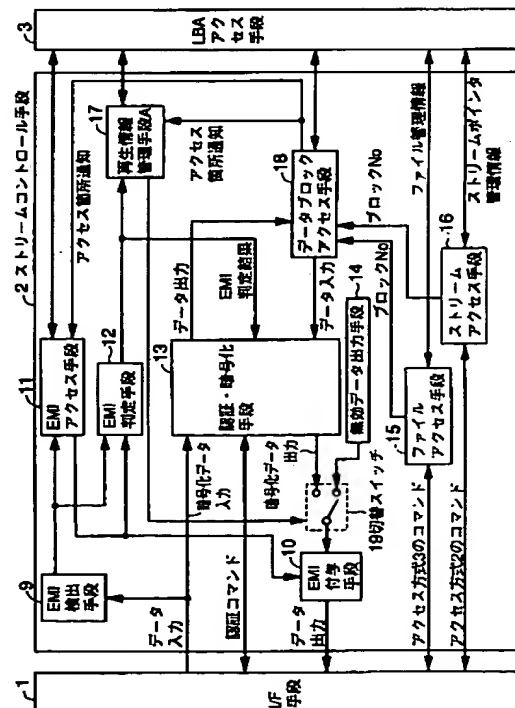
最終頁に続く

(54)【発明の名称】 記録再生装置、プログラム記録媒体及び記録媒体

(57)【要約】

【課題】 放送される番組を一回に限り視聴を許可するというのが著作者の意図である場合に、視聴者が視聴できる時間帯まで限定されてしまう。すなわち視聴者が自分の都合のよい時間帯に番組を視聴したい場合であっても、番組が放送される時間帯にしかその番組を視聴できないという課題がある。

【解決手段】 AVデータを記録する記録手段11、17、18と、前記AVデータの利用許諾情報を示す信号情報が1回だけ視聴を許可する複製禁止 (copy never) を表す場合、記録手段11、17、18により記録されたAVデータを1回だけ再生する再生手段11、17、18、19とを備えたことを特徴とする記録再生装置である。



【特許請求の範囲】

【請求項 1】 AV データを記録する記録手段と、前記 AV データの利用許諾情報を示す信号情報が 1 回だけ視聴することを許可する複製禁止 (copy never) を表す場合、前記記録手段により記録された前記 AV データを 1 回だけ再生する再生手段とを備えたことを特徴とする記録再生装置。

【請求項 2】 AV データを記録する記録手段と、前記 AV データの利用許諾情報を示す信号情報が 1 回だけ複製することを許可する (copy one generation) ことを表す場合、前記記録手段により 1 回複製された後の前記 AV データの前記利用許諾情報を示す信号情報を、再び 1 回だけ複製することを許可する (copy one generation) ことを表して、前記 AV データを 1 回だけ再生する再生手段とを備えたことを特徴とする記録再生装置。

【請求項 3】 前記利用許諾情報は、IEEE 1394 によるパケットのヘッダ内に EMI として保持されており、IEEE 1394 に基づくパケットデータとして送られてくることを特徴とする請求項 1 または 2 記載の記録再生装置。

【請求項 4】 前記利用許諾情報は、IEEE 1394 によるパケットの内部に埋め込まれている CGMS であり、IEEE 1394 に基づくパケットデータとして送られてくることを特徴とする請求項 1 または 2 記載の記録再生装置。

【請求項 5】 前記記録手段は、前記利用許諾情報が複製禁止または 1 回だけ複製許可を表す場合、前記 AV データを記録する際、未再生のデータであることを意味する再生情報を付加し、前記再生手段は、前記利用許諾情報が複製禁止または 1 回だけ複製許可を表す場合、前記 AV データを再生する際、前記 AV データの再生された部分に再生済みであることを意味する前記再生情報を付加し、前記 AV データの未再生の部分と区別することを特徴とする請求項 1 ～ 4 のいずれかに記載の記録再生装置。

【請求項 6】 前記再生手段は、前記利用許諾情報が複製禁止または 1 回だけ複製許可を表す場合、前記 AV データを再生する際、記録媒体上の前記 AV データに関する配置情報を削除してその AV データの占有する領域を空き領域とすることを特徴とする請求項 1 ～ 4 のいずれかに記載の記録再生装置。

【請求項 7】 前記再生手段は、前記利用許諾情報が複製禁止または 1 回だけ複製許可を表す場合、前記 AV データを再生する際、前記 AV データが記録されている記録媒体上の記録部分を消去することを特徴とする請求項 1 ～ 4 のいずれかに記載の記録再生装置。

【請求項 8】 前記記録手段は、前記 AV データと前記再生情報とを同じ領域に関連付けて記録することを特徴とする請求項 5 記載の記録再生装置。

【請求項 9】 前記記録手段は、前記 AV データと前記再生情報とを別々の領域に関連付けて記録することを特徴とする請求項 5 記載の記録再生装置。

【請求項 10】 前記記録手段は、前記再生情報をユーザがアクセス出来ない領域に記録することを特徴とする請求項 5、8 または 9 のいずれかに記載の記録再生装置。

【請求項 11】 請求項 5、8、9 または 10 のいずれかに記載の再生情報を記録していることを特徴とする記録媒体。

【請求項 12】 前記再生手段は、前記 AV データを再生する際、前記利用許諾情報が前記 AV データが複製禁止または 1 回だけ複製許可を表す場合、前記再生情報が前記 AV データの全部または一部が未再生であることを示すとき、その部分の前記 AV データを暗号化して出力することを特徴とする請求項 5、8、9 または 10 のいずれかに記載の記録再生装置。

【請求項 13】 前記再生手段は、前記 AV データを再生する際、前記利用許諾情報が前記 AV データが複製禁止または 1 回だけ再生許可を表す場合、前記再生情報が前記 AV データの全部または一部が再生済みであることを示すとき、その部分の前記 AV データを暗号化して出力し、かつ復号化のための鍵は出力しないことを特徴とする請求項 5、8、9 または 10 のいずれかに記載の記録再生装置。

【請求項 14】 前記再生手段は、前記 AV データを再生する際、前記利用許諾情報が前記 AV データが複製禁止または 1 回だけ複製許可を表す場合、前記再生情報が前記 AV データの全部または一部が再生済みであることを示すとき、その部分の前記 AV データを出力しないで、無効なデータを出力することを特徴とする請求項 5、8、9、10 または 12 のいずれかに記載の記録再生装置。

【請求項 15】 時間とともに変化する一連の鍵を生成する時変鍵生成手段と、

前記鍵を用いて前記 AV データを暗号化する記録用暗号化手段と、

暗号化された前記 AV データを復号化する再生用復号化手段とを有し、

前記 AV データを記録する際、前記利用許諾情報が複製禁止または 1 回だけ複製許可を表す場合、前記記録用暗号化手段は、前記時変鍵生成手段で生成された前記鍵を用いて順次前記 AV データを暗号化し、

前記記録手段は、前記鍵と前記 AV データを関連付けて記録し、

前記 AV データを再生する際、前記利用許諾情報が複製禁止または 1 回だけ複製許可を表す場合、前記再生手段は、暗号化されている前記 AV データと前記鍵とを取り出し、取り出された前記鍵の記録部分を消去し、

前記再生用復号化手段は、取り出された前記鍵を用いて

暗号化されている前記ＡＶデータを復号化することを特徴とする請求項１～４のいずれかに記載の記録再生装置。

【請求項１６】 前記再生手段は、前記鍵の記録部分を消去する際、記録媒体上の鍵に関する記録位置情報を削除することを特徴とする請求項１５記載の記録再生装置。

【請求項１７】 時間とともに変化する一連の鍵を生成する時変鍵生成手段と、

前記鍵を用いて前記ＡＶデータを暗号化する記録用暗号化手段と、

暗号化された前記ＡＶデータを復号化する再生用復号化手段とを有し、

前記ＡＶデータを記録する際、前記利用許諾情報が複製禁止または１回だけ複製許可を表す場合、前記記録用暗号化手段は、前記時変鍵生成手段で生成された前記鍵を用いて順次前記ＡＶデータを暗号化し、

前記記録手段は、前記鍵と前記ＡＶデータを関連付けて記録し、

前記鍵が未だ読み出されていないことを意味する鍵読み出し情報を付加して記録し、

前記ＡＶデータを再生する際、前記利用許諾情報が複製禁止または１回だけ複製許可を表す場合、前記再生手段は、暗号化されている前記ＡＶデータと前記鍵とを取り出し、取り出された前記鍵が読み出し済であることを意味する前記鍵読み出し情報を付加し、

前記再生用復号化手段は、取り出された前記鍵を用いて暗号化されている前記ＡＶデータを復号化することを特徴とする請求項１～４のいずれかに記載の記録再生装置。

【請求項１８】 前記記録手段は、前記鍵または前記鍵読み出し情報を前記ＡＶデータと同じ領域に関連付けて記録することを特徴とする請求項１５または１７記載の記録再生装置。

【請求項１９】 前記記録手段は、前記鍵または前記鍵読み出し情報を前記ＡＶデータと別々の領域に関連付けて記録することを特徴とする請求項１５または１７記載の記録再生装置。

【請求項２０】 前記記録手段は、前記鍵または前記鍵読み出し情報をユーザがアクセスできない領域に記録したことを特徴とする請求項１５、１７、１８または１９のいずれかに記載の記録再生装置。

【請求項２１】 前記ユーザがアクセス出来ない領域とは、ＬＢＡ（logical block address）単位でアクセス出来ない領域、またはＬＢＡ単位でアクセス出来る領域を限定した領域、または交代セクタ領域、またはＡＶデータとして再生される領域以外の領域（ＡＵＸ）、または記録媒体に付加されたＲＡＭ、または光ディスクのヘッダ領域、またはパワーキャリブレーションエリア、またはレコーディングマネージメント

エリア、またはリードインエリア、またはリードアウトエリアであることを特徴とする請求項１０または２０記載の記録再生装置。

【請求項２２】 請求項１７に記載の鍵読み出し情報を記録していることを特徴とする記録媒体。

【請求項２３】 請求項１～２２のいずれかに記載の記録再生装置の各構成要素の全部または一部の機能をコンピュータに実行させるためのプログラムを格納していることを特徴とするプログラム記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＡＶデータにその利用許諾情報が付加されている場合の記録再生装置に関するものである。

【０００２】

【従来の技術】ホーム・マルチメディア・システム、ホーム・ネットワークの要求が、デジタル化の波によって急速に高まってきている。またオフィスや業務システムにおいても家庭のシステム以上にデジタル化とマルチメディア化のニーズが高まっている。このような状況の中にあって近年注目されているのがＩＥＥＥ１３９４－１９９５である。これは、１９９５年にＩＥＥＥで、物理層（Physical Layer）、リンク層（Link Layer）を中心に規格化された高速シリアル・バス標準であり、１００Mbps、２００Mbpsおよび４００Mbpsデータ転送のためのハードウェア、およびソフトウェアの標準である。ＩＥＥＥ１３９４は、プラグ&プレイやマルチメディア・データ転送のための特徴的な機能を備えている。つまりビデオや音声といったデータを転送するための帯域を確保し、リアルタイム転送を可能にするアイソクロナス・データ転送（Isynchronous）を持つ。またＩＥＥＥ１３９４バスで接続されたＰＣの制御プログラムからＩＥＥＥ１３９４制御コマンド（アシンクロナス（非同期）データ）によってデジタルカメラなどの映像データの制御（映像データの切り替え、カメラの制御）を同時に行うこともできる。

【０００３】このような標準であるＩＥＥＥ１３９４－１９５５に基づいて行うＡＶデータの利用許諾情報には、CGMSがある。CGMSは放送局から送られてくるトランスポートストリームの内部に存在している。CGMSは２ビットのデータであり、CGMSの取りうる値とその意味は次のようになる。

【０００４】すなわちCGMS＝１１のときcopy neverを意味し、CGMS＝１０のときcopy one generationを意味し、CGMS＝００のときcopy freeを意味する。ただしcopy neverは複製禁止のことであり、そのＡＶデータを１回だけ視聴することを許可するものである。copy one generationは１世代のみ

複製を許可するものであり、複製したAVデータは何度でも繰り返して視聴することができるものである。copy freeは自由に複製してよいことを示すものである。

【0005】CGMSが11のときすなわちcopy neverのとき、AVデータは一回だけ視聴することが出来る。すなわちそのAVデータが放送されている時間帯に限ってそのAVデータを視聴することができる。

【0006】

【発明が解決しようとする課題】しかし、従来、CGMSによる利用許諾情報がcopy neverの場合は該当するAVデータを一回だけ視聴することができるが、視聴できる時間帯は番組が放送されている時間帯に限られていた。このように一回だけ視聴を許可するというのが著作権者の意図である場合に視聴できる時間帯まで限定されてしまう。すなわち視聴者が自分の都合のよい時間帯に番組を視聴したい場合であっても、番組が放送される時間帯にしかその番組を視聴できないという課題がある。

【0007】またCGMSによる利用許諾情報がcopy one generationの場合に、一度ある記録媒体に記録してしまうと、その他の記録媒体へAVデータを移動することができないという課題がある。

【0008】本発明は番組の利用許諾情報を表す情報が複製禁止の場合に、一回だけ視聴を許可するという著作権者の意図通りに視聴者がAVデータを視聴でき、かつそのAVデータが放送された以後で時間帯を限定されずにそのAVデータを視聴者が視聴できる記録再生装置及びプログラム記録媒体を提供することを目的とするものである。

【0009】また本発明は番組の利用許諾情報が一回だけ複製を許可する場合に、一度記録した記録媒体から別の記録媒体へAVデータの移動を行うことが出来る記録再生装置及びプログラム記録媒体を提供することを目的とするものである。

【0010】

【課題を解決するための手段】上述した課題を解決するために、第1の本発明（請求項1に対応）は、AVデータを記録する記録手段と、前記AVデータの利用許諾情報を示す信号情報が1回だけ視聴することを許可する複製禁止（copy never）を表す場合、前記記録手段により記録された前記AVデータを1回だけ再生する再生手段とを備えたことを特徴とする記録再生装置である。

【0011】また第2の本発明（請求項2に対応）は、AVデータを記録する記録手段と、前記AVデータの利用許諾情報を示す信号情報が1回だけ複製することを許可する（copy one generation）ことを表す場合、前記記録手段により1回複製された後の前記AVデータの前記利用許諾情報を示す信号情報を、

再び1回だけ複製することを許可する（copy one generation）ことを表して、前記AVデータを1回だけ再生する再生手段とを備えたことを特徴とする記録再生装置である。

【0012】また第3の本発明（請求項3に対応）は、前記利用許諾情報は、IEEE1394によるパケットのヘッダ内にEMIとして保持されており、IEEE1394に基づくパケットデータとして送られてくることを特徴とする第1または2の発明に記載の記録再生装置である。

【0013】また第4の本発明（請求項4に対応）は、前記利用許諾情報は、IEEE1394によるパケットの内部に埋め込まれているCGMSであり、IEEE1394に基づくパケットデータとして送られてくることを特徴とする第1または2の発明に記載の記録再生装置である。

【0014】また第5の本発明（請求項5に対応）は、前記記録手段は、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記AVデータを記録する際、未再生のデータであることを意味する再生情報を付加し、前記再生手段は、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記AVデータを再生する際、前記AVデータの再生された部分に再生済みであることを意味する前記再生情報を付加し、前記AVデータの未再生の部分と区別することを特徴とする第1～4の発明のいずれかに記載の記録再生装置である。

【0015】また第6の本発明（請求項6に対応）は、前記再生手段は、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記AVデータを再生する際、記録媒体上の前記AVデータに関する配置情報を削除してそのAVデータの占有する領域を空き領域とすることを特徴とする第1～4の発明のいずれかに記載の記録再生装置である。

【0016】また第7の本発明（請求項7に対応）は、前記再生手段は、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記AVデータを再生する際、前記AVデータが記録されている記録媒体上の記録部分を消去することを特徴とする第1～4の発明のいずれかに記載の記録再生装置である。

【0017】また第8の本発明（請求項8に対応）は、前記記録手段は、前記AVデータと前記再生情報とを同じ領域に関連付けて記録することを特徴とする第5の発明に記載の記録再生装置である。

【0018】また第9の本発明（請求項9に対応）は、前記記録手段は、前記AVデータと前記再生情報とを別々の領域に関連付けて記録することを特徴とする第5の発明に記載の記録再生装置である。

【0019】また第10の本発明（請求項10に対応）は、前記記録手段は、前記再生情報をユーザがアクセス出来ない領域に記録することを特徴とする第5、8また

は 9 の発明のいずれかに記載の記録再生装置である。

【0020】また第 11 の本発明（請求項 11 に対応）は、第 5、8、9 または 10 の発明のいずれかに記載の再生情報を記録していることを特徴とする記録媒体である。

【0021】また第 12 の本発明（請求項 12 に対応）は、前記再生手段は、前記 A V データを再生する際、前記利用許諾情報が前記 A V データが複製禁止または 1 回だけ複製許可を表す場合、前記再生情報が前記 A V データの全部または一部が未再生であることを示すとき、その部分の前記 A V データを暗号化して出力することを特徴とする第 5、8、9 または 10 の発明のいずれかに記載の記録再生装置である。

【0022】また第 13 の本発明（請求項 13 に対応）は、前記再生手段は、前記 A V データを再生する際、前記利用許諾情報が前記 A V データが複製禁止または 1 回だけ再生許可を表す場合、前記再生情報が前記 A V データの全部または一部が再生済であることを示すとき、その部分の前記 A V データを暗号化して出力し、かつ復号化のための鍵は出力しないことを特徴とする第 5、8、9 または 10 の発明のいずれかに記載の記録再生装置である。

【0023】また第 14 の本発明（請求項 14 に対応）は、前記再生手段は、前記 A V データを再生する際、前記利用許諾情報が前記 A V データが複製禁止または 1 回だけ複製許可を表す場合、前記再生情報が前記 A V データの全部または一部が再生済みであることを示すとき、その部分の前記 A V データを出力しないで、無効なデータを出力することを特徴とする第 5、8、9、10 または 12 の発明のいずれかに記載の記録再生装置である。

【0024】第 15 の本発明（請求項 15 に対応）は、時間とともに変化する一連の鍵を生成する時変鍵生成手段と、前記鍵を用いて前記 A V データを暗号化する記録用暗号化手段と、暗号化された前記 A V データを復号化する再生用復号化手段とを有し、前記 A V データを記録する際、前記利用許諾情報が複製禁止または 1 回だけ複製許可を表す場合、前記記録用暗号化手段は、前記時変鍵生成手段で生成された前記鍵を用いて順次前記 A V データを暗号化し、前記記録手段は、前記鍵と前記 A V データを関連付けて記録し、前記 A V データを再生する際、前記利用許諾情報が複製禁止または 1 回だけ複製許可を表す場合、前記再生手段は、暗号化されている前記 A V データと前記鍵とを取り出し、取り出された前記鍵の記録部分を消去し、前記再生用復号化手段は、取り出された前記鍵を用いて暗号化されている前記 A V データを復号化することを特徴とする第 1～4 の発明のいずれかに記載の記録再生装置である。

【0025】また第 16 の本発明（請求項 16 に対応）は、前記再生手段は、前記鍵の記録部分を消去する際、

記録媒体上の鍵に関する記録位置情報を削除することを特徴とする請求項 15 記載の記録再生装置である。

【0026】また第 17 の本発明（請求項 17 に対応）は、時間とともに変化する一連の鍵を生成する時変鍵生成手段と、前記鍵を用いて前記 A V データを暗号化する記録用暗号化手段と、暗号化された前記 A V データを復号化する再生用復号化手段とを有し、前記 A V データを記録する際、前記利用許諾情報が複製禁止または 1 回だけ複製許可を表す場合、前記記録用暗号化手段は、前記時変鍵生成手段で生成された前記鍵を用いて順次前記 A V データを暗号化し、前記記録手段は、前記鍵と前記 A V データを関連付けて記録し、前記鍵が未だ読み出されていないことを意味する鍵読み出し情報を付加して記録し、前記 A V データを再生する際、前記利用許諾情報が複製禁止または 1 回だけ複製許可を表す場合、前記再生手段は、暗号化されている前記 A V データと前記鍵とを取り出し、取り出された前記鍵が読み出し済であることを意味する前記鍵読み出し情報を付加し、前記再生用復号化手段は、取り出された前記鍵を用いて暗号化されている前記 A V データを復号化することを特徴とする第 1～4 の発明のいずれかに記載の記録再生装置である。

【0027】また第 18 の本発明（請求項 18 に対応）は、前記記録手段は、前記鍵または前記鍵読み出し情報を前記 A V データと同じ領域に関連付けて記録することを特徴とする第 15 または 17 の発明に記載の記録再生装置である。

【0028】また第 19 の本発明（請求項 19 に対応）は、前記記録手段は、前記鍵または前記鍵読み出し情報を前記 A V データと別々の領域に関連付けて記録することを特徴とする第 15 または 17 の発明に記載の記録再生装置である。

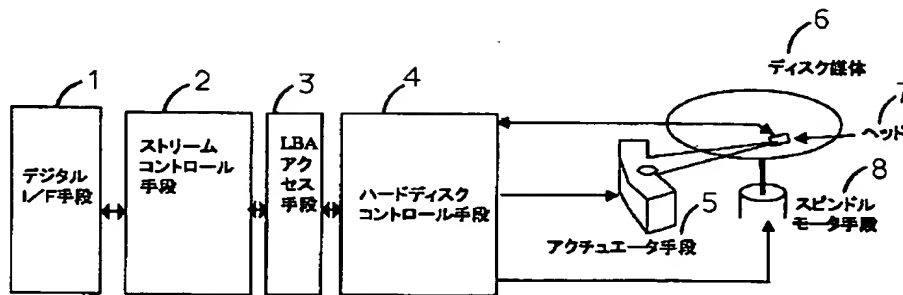
【0029】また第 20 の本発明（請求項 20 に対応）は、前記記録手段は、前記鍵または前記鍵読み出し情報をユーザがアクセスできない領域に記録したことを特徴とする第 15、17、18 または 19 の発明のいずれかに記載の記録再生装置である。

【0030】また第 21 の本発明（請求項 21 に対応）は、前記ユーザがアクセス出来ない領域とは、LBA（logical block address）単位でアクセス出来ない領域、または LBA 単位でアクセス出来る領域を限定した領域、または交代セクタ領域、または A V データとして再生される領域以外の領域（AUX）、または記録媒体に付加された RAM、または光ディスクのヘッダ領域、またはパワーキャリブレーションエリア、またはレコーディングマネジメントエリア、またはリードインエリア、またはリードアウトエリアであることを特徴とする第 10 または 20 の発明に記載の記録再生装置である。

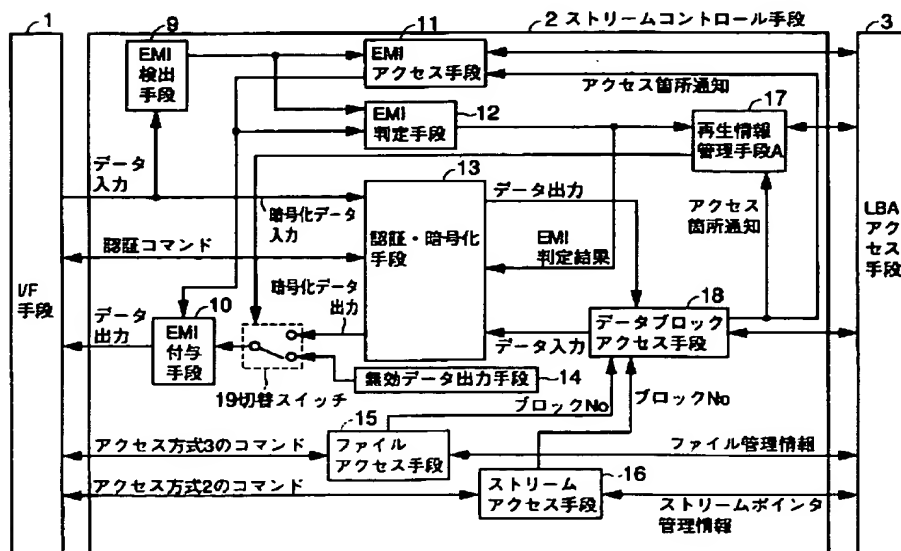
【0031】また第 22 の本発明（請求項 22 に対応）は、第 17 の発明に記載の鍵読み出し情報を記録してい

- | | |
|------------------|---------------|
| 9 EMI検出手段 | 20 復号化手段 |
| 10 EMI付与手段 | 21 認証手段 |
| 11 EMIアクセス手段 | 22 鍵生成手段 |
| 12 EMI判定手段 | 23 暗号化手段 |
| 13 認証・暗号化手段 | 24 切替スイッチ |
| 14 無効データ出力手段 | 25 切替スイッチ |
| 15 ファイルアクセス手段 | 26 再生情報更新手段 |
| 16 ストリームアクセス手段 | 27 再生済判定手段 |
| 17 再生情報管理手段A | 28 再生情報生成手段 |
| 18 データブロックアクセス手段 | 29 再生情報アクセス手段 |
| 19 切替スイッチ | 30 切替スイッチ |

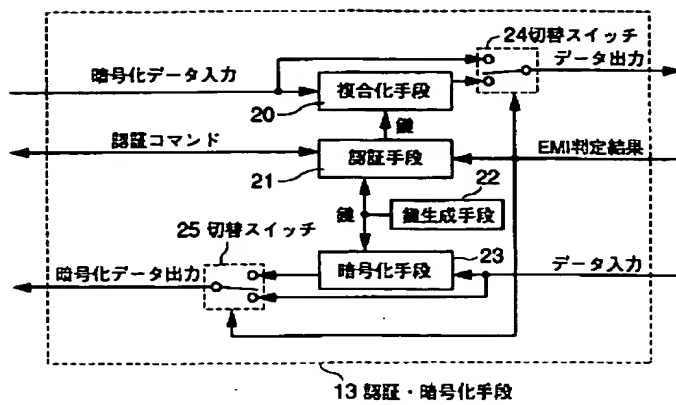
【図1】



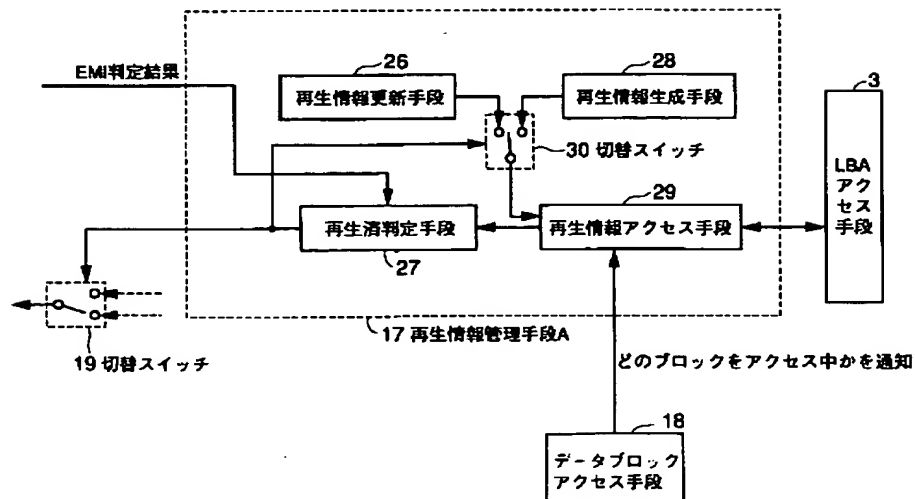
【図2】



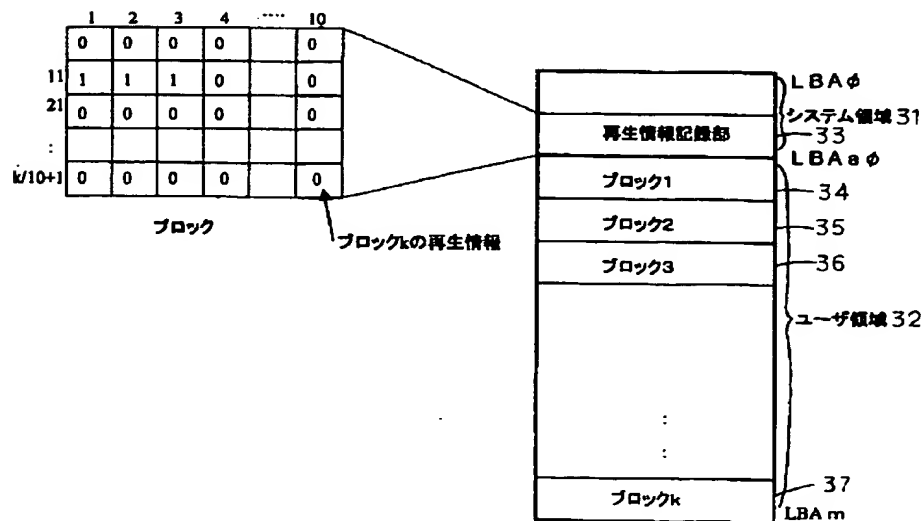
【図3】



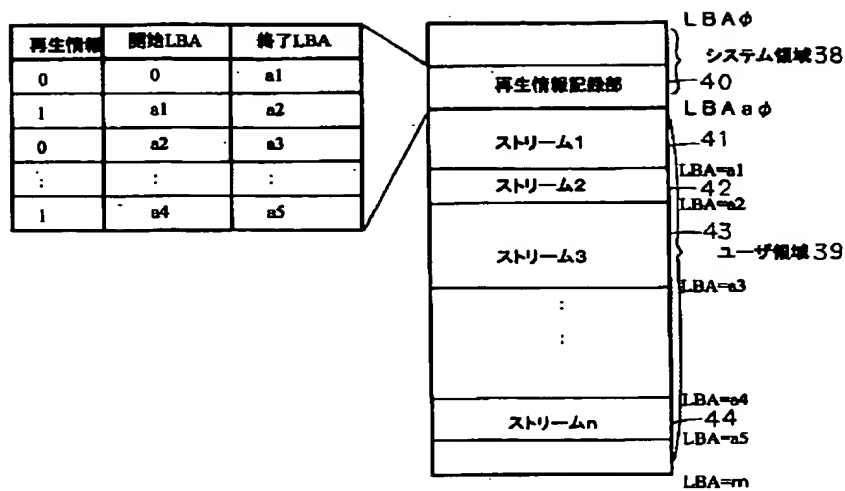
【図4】



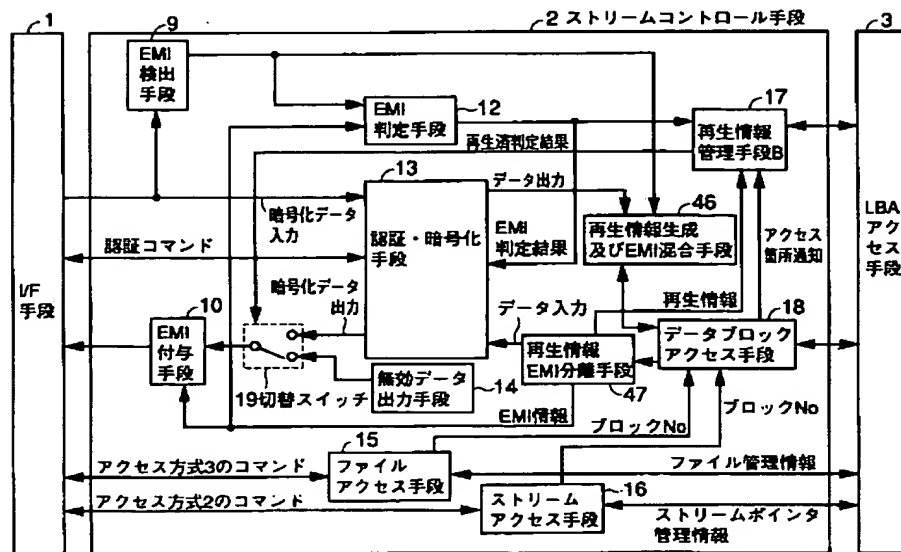
【図5】



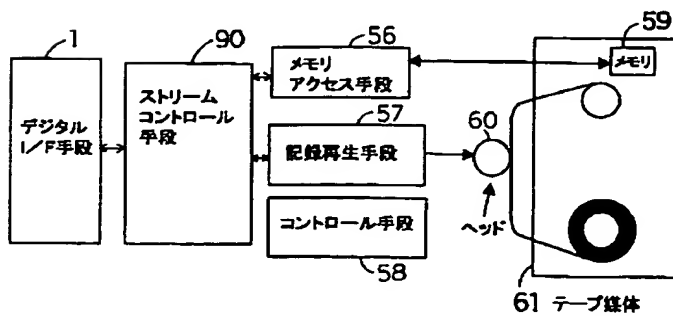
【図6】



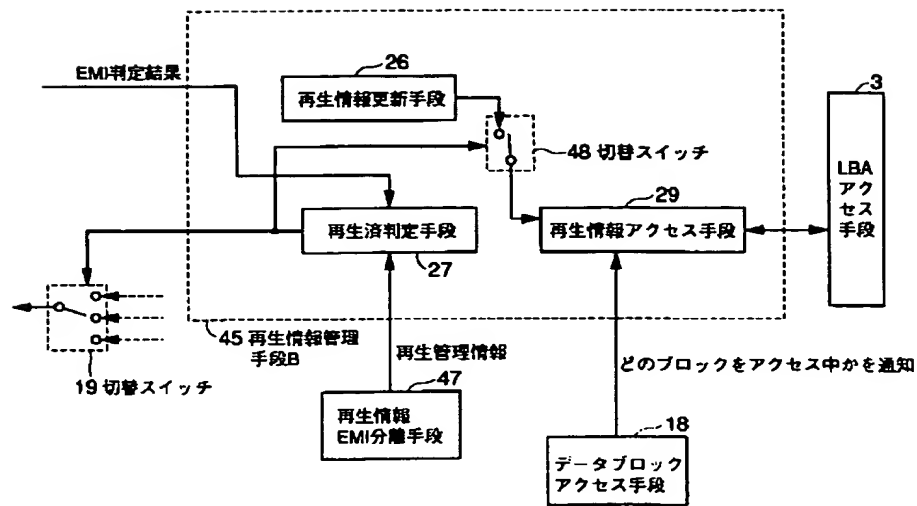
【図7】



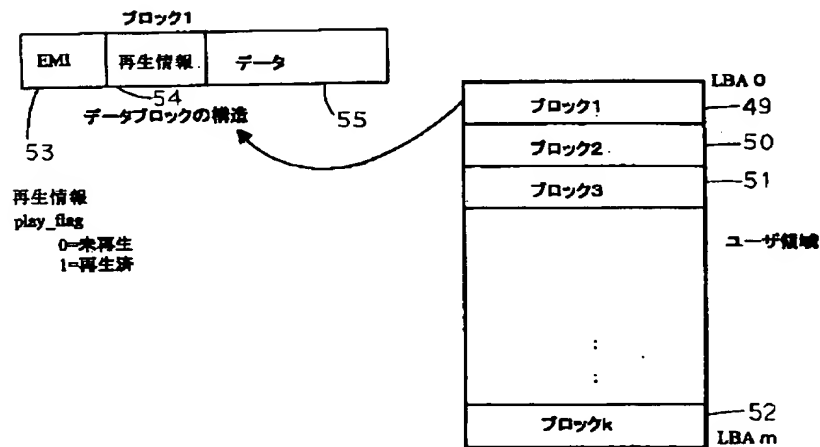
【図12】



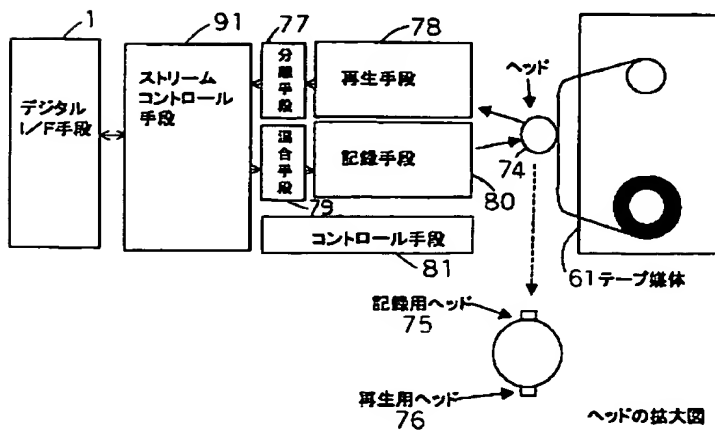
【図8】



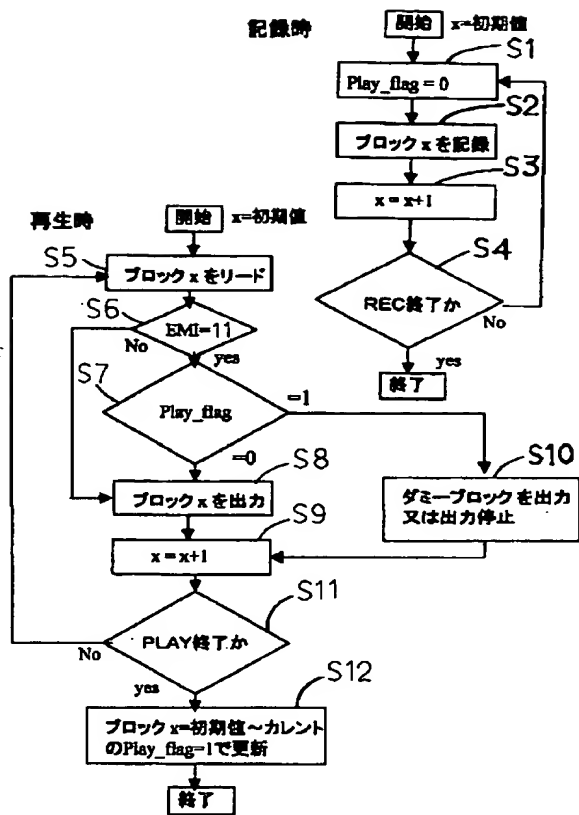
【図9】



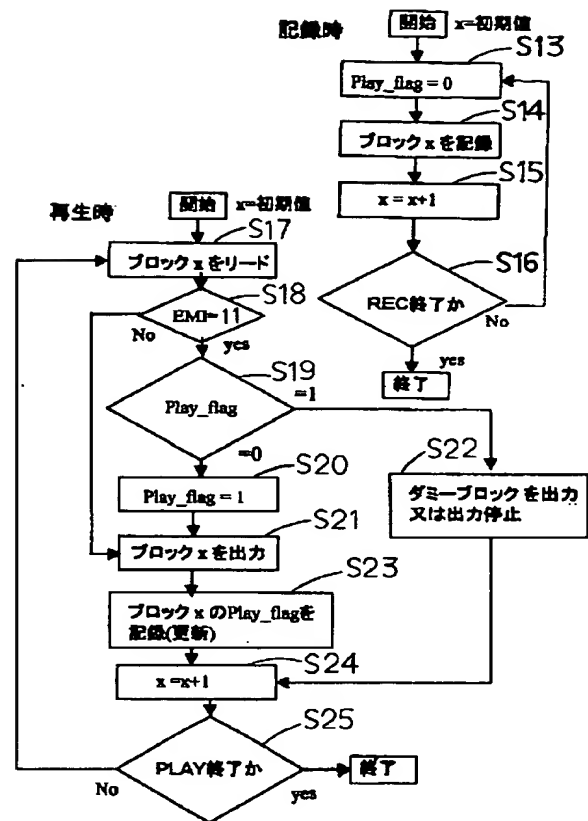
【図16】



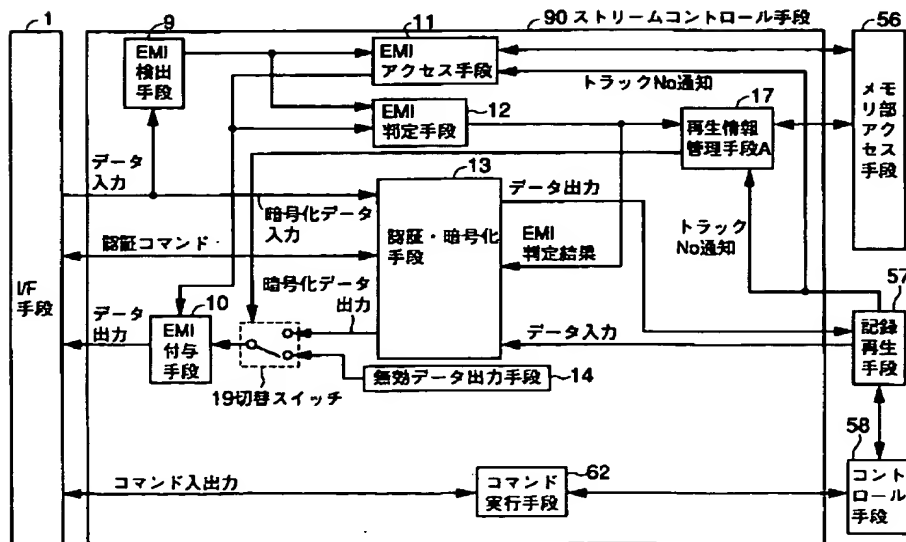
【図10】



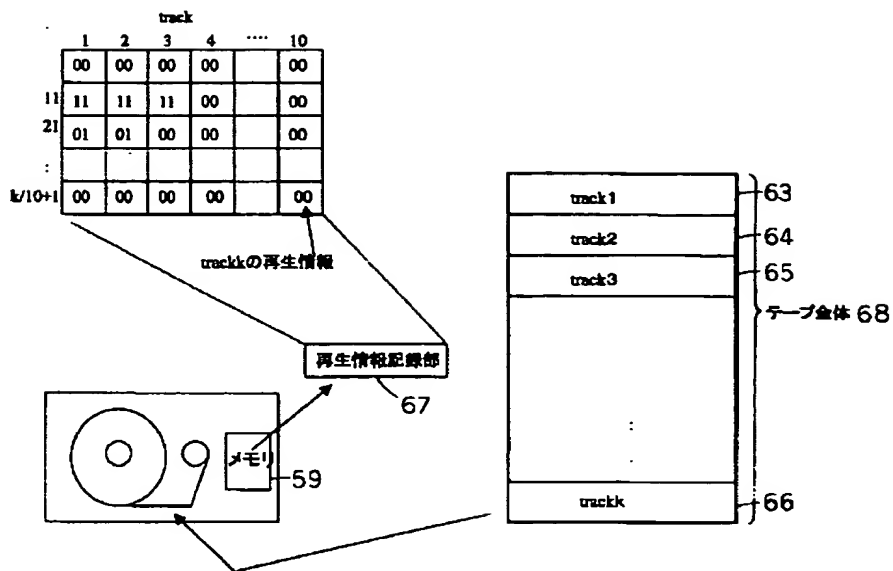
【図11】



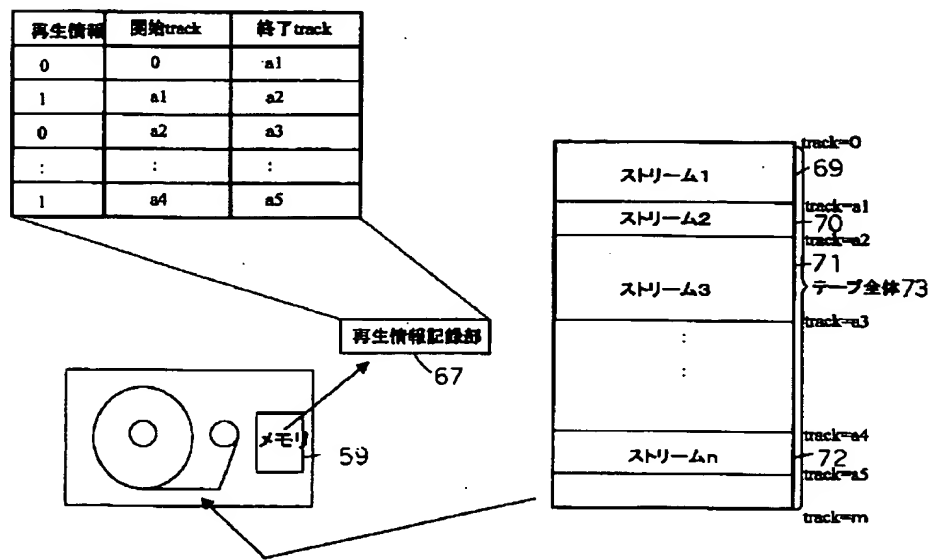
【図13】



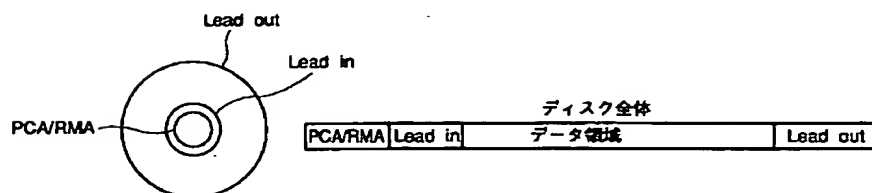
【図14】



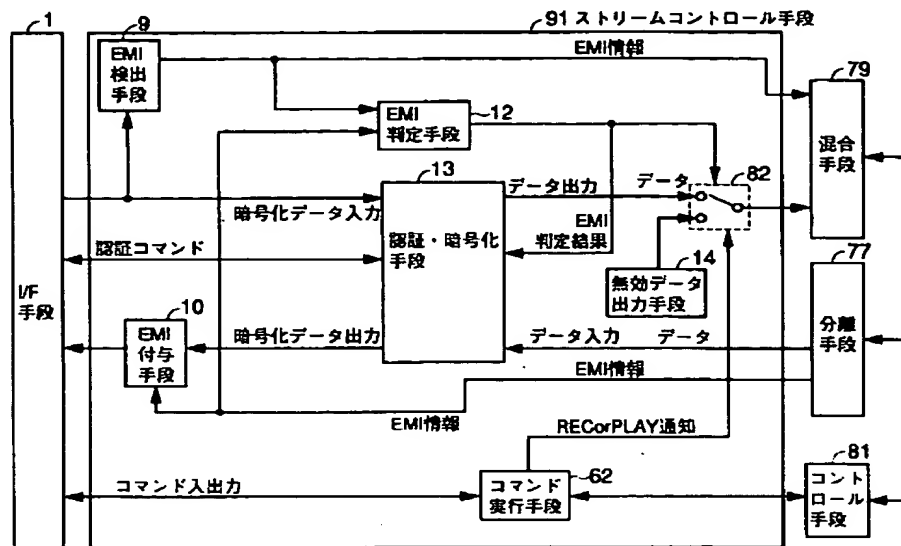
【図15】



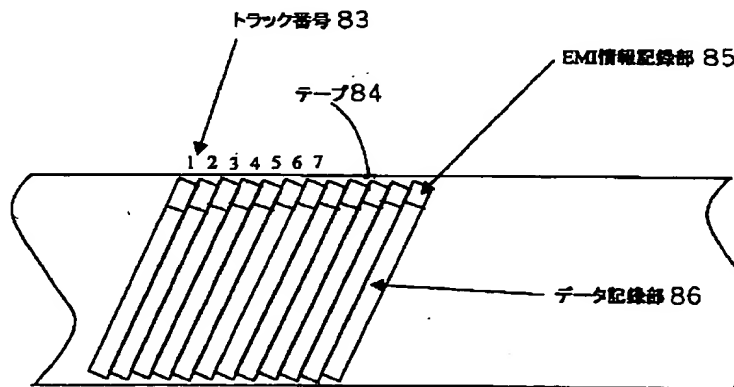
【図24】



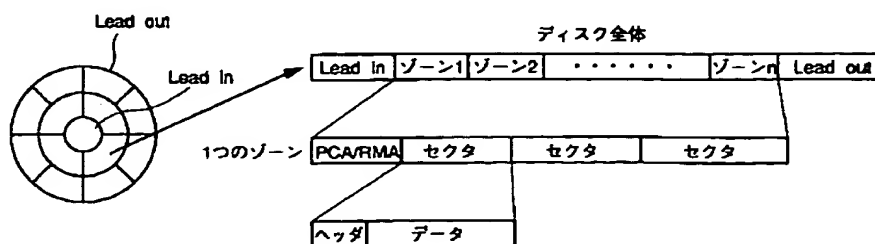
【図17】



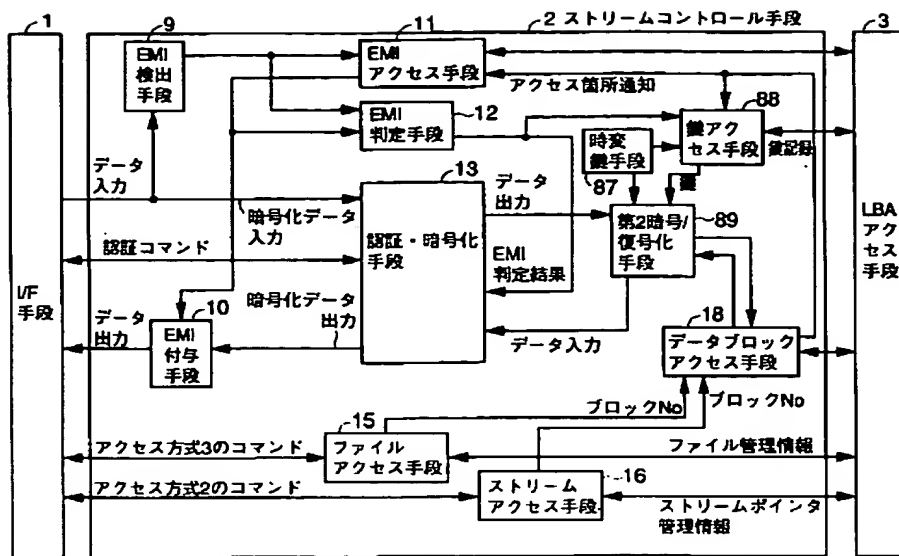
【図18】



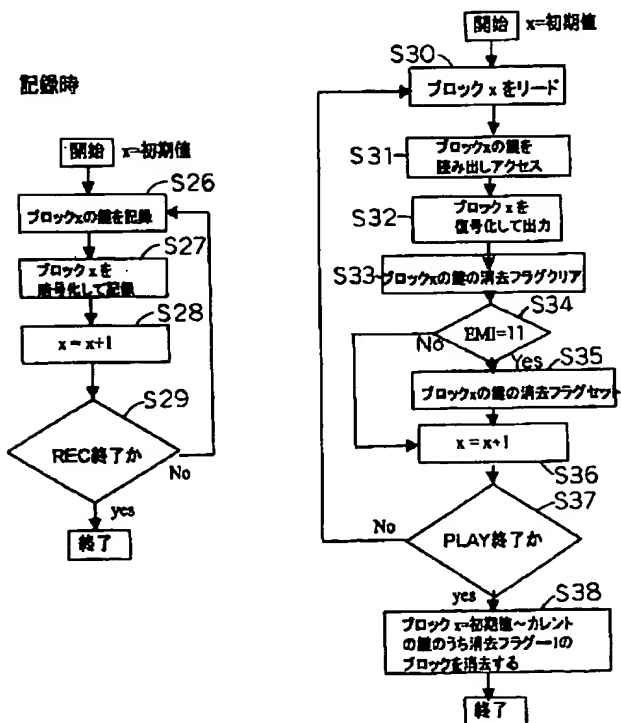
【図25】



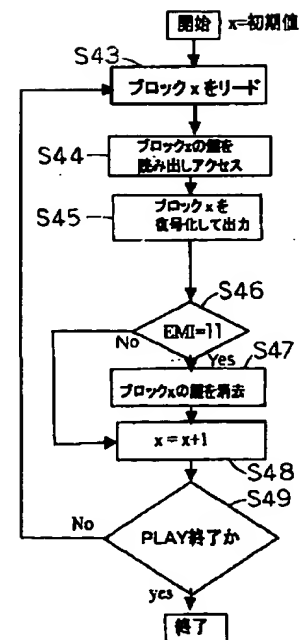
【図19】



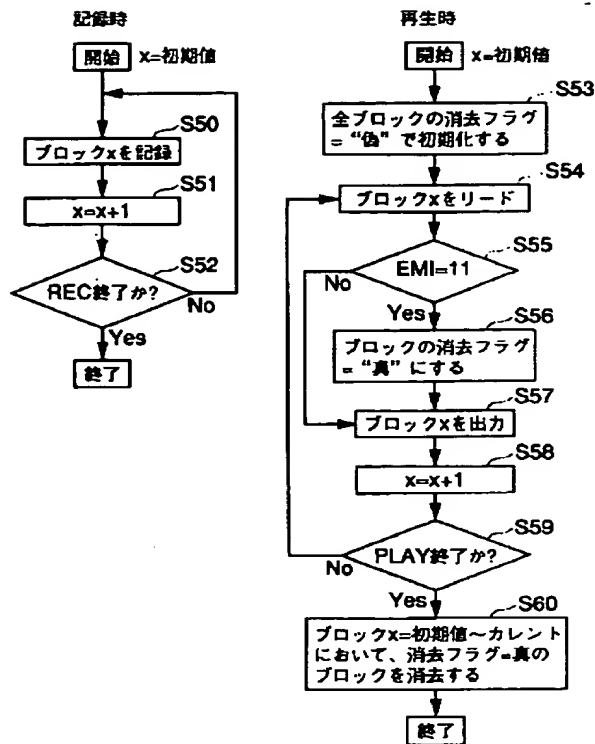
【図20】



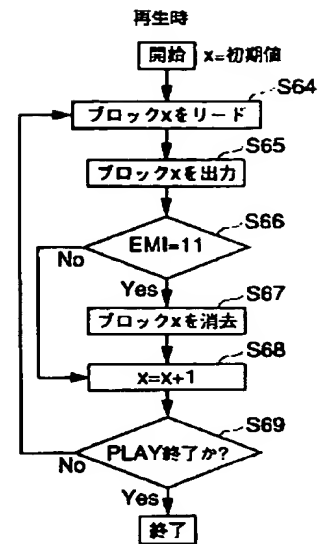
【図21】



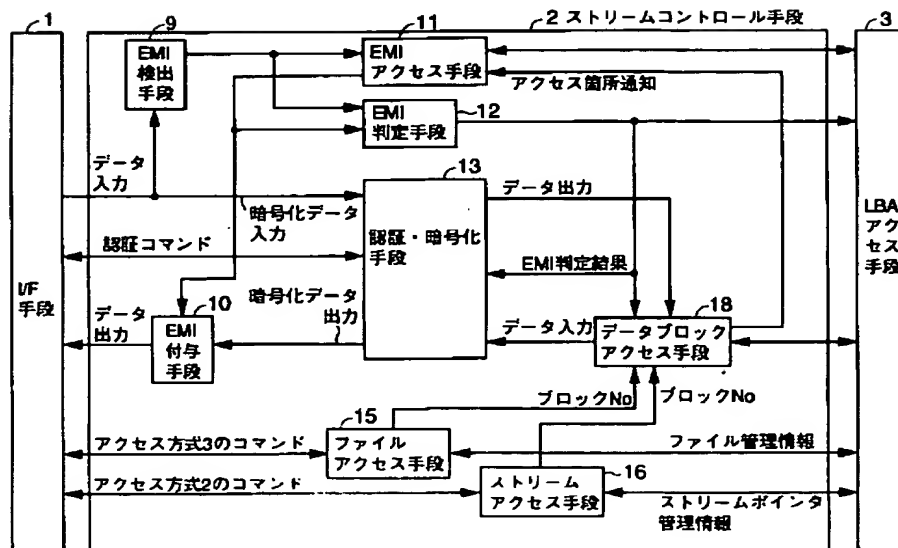
【図22】



【図23】



【図26】



E6303-01

- 1 -

[TITLE OF THE INVENTION]

RECORDING AND REPRODUCING APPARATUS, PROGRAM
RECORDING MEDIUM AND RECORDING MEDIUM



[ABSTRACT]

[Problem]

In the case where a copyright holder's intention is to permit a viewer to view a broadcast program once, the viewer will have a limitation for a time when the broadcast program is broadcasted. In other words, there is a problem that the user can view the program only when the program is actually broadcasted even if the viewer desires to view the program during a period of time convenient for the viewer.

[Solving Means]

A recording and reproducing apparatus characterized by comprising recording means 11, 17 and 18 for recording AV data and reproducing means 11, 17, 18 and 19 for reproducing once the AV data that are recorded by the recording means 11, 17 and 18 in the case where signal information indicating licensing information of the AV data represents a prohibition of copying (copy never) that means a permission of a onetime-only viewing.

[What is claimed is:]

[Claim 1]

A recording and reproducing apparatus characterized by comprising:

a recording means for recording AV data; and

a reproducing means for reproducing the AV data once that is recorded by the recording means, in the case where an information signal indicating licensing information of the AV data represents a prohibition of copying (copy never) that means a permission of a one-time-only viewing.

[Claim 2]

A recording and reproducing apparatus characterized by comprising:

a recording means for recording AV data; and

in the case where an information signal indicating licensing information of the AV data represents a permission of copying once (copy one generation), a reproducing means for representing a second-time permission of copying once (copy one generation) for the information signal that indicates the licensing information of the AV data after being copied once by the recording means, and for reproducing once the AV data.

[Claim 3]

The recording and reproducing apparatus according to Claim 1 or 2, wherein the licensing information is an EMI

that is retained inside a header of a packet according to IEEE 1394 and is sent as packet data based on the IEEE 1394.
[Claim 4]

The recording and reproducing apparatus according to Claim 1 or 2, wherein the licensing information is CGMS that is embedded inside a packet according to IEEE 1394 and is sent as a data packet based on the IEEE 1394.
[Claim 5]

The recording and reproducing apparatus according to any one of Claims 1 to 4, characterized in that, in the case where the licensing information represents a prohibition of copying or a permission of copying once, the recording means adds reproduction information indicating that the AV data has been non-reproduced data when recording the AV data, and

in the case where the licensing information represents a prohibition of copying or a permission of copying once, the reproducing means adds to a reproduced portion of the AV data the reproduction information indicating that the portion has been reproduced when reproducing the AV data so as to distinguish the reproduced portion from a non-reproduced portion of the AV data.

[Claim 6]

The recording and reproducing apparatus according to any one of Claims 1 to 4, characterized in that, in the

case where the licensing information represents a prohibition of copying or a permission of copying once, the reproducing means deletes positional information of the AV data on a recording medium when reproducing the AV data to make an area occupied by the AV data to be a free area.

[Claim 7]

The recording and reproducing apparatus according to any one of Claims 1 to 4, characterized in that, in the case where the licensing information represents a prohibition of copying or a permission of copying once, the reproducing means erases a recorded portion on a recording medium where the AV data is recorded when reproducing the AV data.

[Claim 8]

The recording and reproducing apparatus according to Claim 5, characterized in that the recording means records the AV data and the reproduction information with the data and the information being associated with each other in an identical area.

[Claim 9]

The recording and reproducing apparatus according to Claim 5, characterized in that the recording means records the AV data and the reproduction information with the data and the information being associated with each other in separate areas.

[Claim 10]

The recording and reproducing apparatus according to any one of Claims 5, 8 and 9, characterized in that the recording means records the reproduction information in an area that a user cannot access.

[Claim 11]

A recording medium characterized by recording the reproduction information according to any one of Claims 5, 8, 9 and 10.

[Claim 12]

The recording and reproducing apparatus according to any one of Claims 5, 8, 9 and 10, characterized in that, if the reproduction information indicates that whole or a portion of the AV data has been non-reproduced in the case where the licensing information represents a prohibition of copying or a permission of copying once, the reproducing means outputs the whole or the portion of the AV data after encrypting the whole or the portion at the time of reproducing the AV data.

[Claim 13]

The recording and reproducing apparatus according to any one of Claims 5, 8, 9 and 10, characterized in that, if the reproduction information indicates that whole or a portion of the AV data has been reproduced in the case where the licensing information represents a prohibition of

copying or a permission of copying once, the reproducing means outputs the whole or the portion of the AV data after encrypting the whole or the portion of the AV data and does not output a key for decryption at the time of reproducing the AV data.

[Claim 14]

The recording and reproducing apparatus according to any one of Claims 5, 8, 9, 10 and 12 characterized in that, if the reproduction information indicates that whole or a portion of the AV data has been reproduced in the case where the licensing information represents a prohibition of copying or a permission of copying once, the reproducing means does not output the whole or the portion of the AV data and outputs invalid data at the time of reproducing the AV data.

[Claim 15]

The recording and reproducing apparatus according to any one of Claims 1 to 4, characterized by comprising:

a time-variant key generating means for generating a series of keys each of which varies with time;

a recording encrypting means for encrypting the AV data by using the keys; and

a reproducing decrypting means for decrypting the encrypted AV data;

wherein:

the recording encrypting means encrypts the AV data sequentially by using the keys generated by the time-variant key generating means when recording the AV data in the case where the licensing information represents a prohibition of copying or a permission of copying once;

the recording means records the keys and the AV data in association with each other;

the reproducing means takes out the encrypted AV data and the keys and erases the recorded portion of the taken out keys when reproducing the AV data in the case where the licensing information represents a prohibition of copying or a permission of copying once; and

the reproducing decrypting means decrypts the encrypted AV data by using the taken out keys.

[Claim 16]

The recording and reproducing apparatus according to Claim 15, characterized in that the reproducing means deletes recorded positional information with respect to a key in a recording medium when erasing the recording portion of the keys.

[Claim 17]

The recording and reproducing apparatus according to any one of Claims 1 to 4, characterized by comprising:

a time-variant key generating means for generating a series of keys each of which varies with time;

a recording encrypting means for encrypting the AV data by using the keys; and

a reproducing decrypting means for decrypting the encrypted AV data;

wherein:

the recording encrypting means encrypts the AV data sequentially by using the keys generated by the time-variant key generating means when recording the AV data in the case where the licensing information represents a prohibition of copying or a permission of copying once;

the recording means records the keys and the AV data in association with each other;

the recording is performed with adding key retrieving information indicating that the keys are not retrieved yet;

the reproducing means takes out the encrypted AV data and the keys and adds thereto the key retrieving information indicating that the taken out keys have been retrieved when reproducing the AV data in the case where the licensing information represents a prohibition of copying or a permission of copying once; and

the reproducing decrypting means decrypts the encrypted AV data by using the taken out keys.

[Claim 18]

The recording and reproducing apparatus according to

Claim 15 or 17, characterized in that the recording means records the keys or the key retrieving information with the keys or the information being associated with each other in a same area as that of the AV data.

[Claim 19]

The recording and reproducing apparatus according to Claim 15 or 17, characterized in that the recording means records the keys or the key retrieving information with the keys or the information being associated with each other in separate areas from that of the AV data.

[Claim 20]

The recording and reproducing apparatus according to any one of Claims 15, 17, 18 and 19, characterized in that the recording means records the keys or the key retrieving information in an area that a user cannot access.

[Claim 21]

The recording and reproducing apparatus according to Claim 10 or 20, characterized in that the area that a user cannot access is an area that cannot be accessed via LBA (logical block address) unit, an area wherein an area that can be accessed via the LBA unit is limited, an alternating sector area, an area other than an area to be reproduced as AV data (AUX), a RAM that is added to a recording medium, a header area of an optical disk, a power calibration area, a recording management area, a lead-in area or a lead-out

area.

[Claim 22]

A recording medium characterized by recording the keys retrieving information according to Claim 17.

[Claim 23]

A program recording medium characterized by storing a program for letting a computer execute whole or a portion of functions of elements for the recording and reproducing apparatus according to any one of Claims 1 to 22.

[Detailed Description of the Invention]

[0001]

[Technical Field to Which the Invention Pertains]

The present invention relates to a recording and reproducing apparatus in the case where AV data is accompanied by licensing information thereof.

[0002]

[Prior Art]

A demand for home multimedia system and home networking is growing rapidly through the influence of digitalization. Also, there is an increasing need of digitalization and multimedia presentation in offices or business systems more than the systems at home. Under the circumstances, IEEE 1394-1995 recently attracts attention. This is a serial bus standard normalized by IEEE mainly for the physical layer and the link layer, and is a standard

for hardware and software used for transmitting 100 Mbps, 200 Mbps and 400 Mbps data. The IEEE 1394 is provided with a characteristic function for the plug & play and multimedia data transmission. Namely, The IEEE 1394 includes an isochronous data transmission that secures bandwidths for transmitting data such as video or sound and that enables real-time transmission. Further, it is possible to simultaneously control image data such as those captured by a digital camera (switching of image data, camera control) by using an IEEE 1394 control command (asynchronous data) from a control program of a PC that is connected via an IEEE 1394 bus.

[0003]

CGMS is licensing information of AV data that is generated based on the IEEE 1394-1955 standard. The CGMS exists in a transport stream broadcasted from a broadcasting station. The CGMS is a 2-bit data, and values and meaning thereof are as follows.

[0004]

It means "copy never" when CGMS = 11; it means "copy one generation" when CGMS = 10; and it means "copy free" when CGMS = 00. Note that "copy never" means a prohibition of copying and permission of viewing the AV data once. "Copy one generation" means that one generation copying is permitted and that the copied AV data can be viewed for a

plurality of times. "Copy free" indicates a liberty of copying.

[0005]

When CGMS = 11, i.e., "copy never", AV data is viewed once. That is to say, one can view the AV data only when the AV data is broadcasted.

[0006]

[Problem to be Solved by the Invention]

Conventionally, the AV data can be viewed once when the licensing information via CGMS is "copy never", but a time in which a program can be viewed is limited to the time of broadcasting of the program. Thus, in the case where a copyright holder's intention is to permit a viewer to view a broadcast program once, the viewer will have a limitation for a time when the broadcast program is broadcasted. In other words, there is a problem that the user cannot choose but view the program at the time when the program is actually broadcasted even when the viewer wants to view the program at a time convenient for the viewer.

[0007]

Further, in the case where the licensing information according to the CGMS is "copy one generation", there is a problem that AV data cannot be transferred to other recording media if the AV data is once recorded in a

recording medium.

[0008]

An object of the present invention is to provide a recording and reproducing apparatus and a program recording medium that enable a viewer to view AV data in accordance with the copyright holder's intention to permit one-time-only viewing and at a time after the AV data is broadcasted without a limitation on time in the case where information representing the licensing information of a program is a prohibition of copying.

[0009]

Another object of the present invention is to provide a recording and reproducing apparatus and a program recording medium that enable AV data to be transferred from a recording medium wherein the AV data is recorded once to another recording medium in the case where the licensing information of a program permits a one-time-only copying.

[0010]

[Means for Solving the Problems]

In order to solve above problems, a first invention (corresponding to Claim 1) is a recording and reproducing apparatus characterized by comprising: a recording means for recording AV data; and a reproducing means for reproducing the AV data once that is recorded by the recording means, in the case where an information signal

indicating licensing information of the AV data represents a prohibition of copying (copy never) that means a permission of a one-time-only viewing.

[0011]

A second invention (corresponding to Claim 2) is a recording and reproducing apparatus characterized by comprising: a recording means for recording AV data; and in the case where an information signal indicating licensing information of the AV data represents a permission of copying once (copy one generation), a reproducing means for representing a second-time permission of copying once (copy one generation) for the information signal that indicates the licensing information of the AV data after being copied once by the recording means, and for reproducing once the AV data.

[0012]

A third invention (corresponding to Claim 3) is the recording and reproducing apparatus according to the first or the second invention, which is characterized in that the licensing information is an EMI that is retained inside a header of a packet according to IEEE 1394 and is sent as packet data based on the IEEE 1394.

[0013]

A fourth invention (corresponding to Claim 4) is the recording and reproducing apparatus according to the first

or second invention, which is characterized in that the licensing information is CGMS that is embedded inside a packet according to IEEE 1394 and is sent as a data packet based on the IEEE 1394.

[0014]

A fifth invention (corresponding to Claim 5) is the recording and reproducing apparatus according to any one of the first to fourth inventions, which is characterized in that, in the case where the licensing information represents a prohibition of copying or a permission of copying once, the recording means adds reproduction information indicating that the AV data has been non-reproduced data when recording the AV data, and in the case where the licensing information represents a prohibition of copying or a permission of copying once, the reproducing means adds to a reproduced portion of the AV data the reproduction information indicating that the portion has been reproduced when reproducing the AV data so as to distinguish the reproduced portion from a non-reproduced portion of the AV data.

[0015]

A sixth invention (corresponding to Claim 6) is the recording and reproducing apparatus according to any one of the first to fourth inventions, which is characterized in that, in the case where the licensing information

represents a prohibition of copying or a permission of copying once, the reproducing means deletes positional information of the AV data on a recording medium when reproducing the AV data to make an area occupied by the AV data to be a free area.

[0016]

A seventh invention (corresponding to Claim 7) is the recording and reproducing apparatus according to any one of the first to fifth inventions, which is characterized in that, in the case where the licensing information represents a prohibition of copying or a permission of copying once, the reproducing means erases a recorded portion on a recording medium where the AV data is recorded when reproducing the AV data.

[0017]

An eighth invention (corresponding to Claim 8) is the recording and reproducing apparatus according to the fifth invention, which is characterized in that the recording means records the AV data and the reproduction information with the data and the information being associated with each other in an identical area.

[0018]

A ninth invention (corresponding to Claim 9) is the recording and reproducing apparatus according to the fifth invention, which is characterized in that the recording

means records the AV data and the reproduction information with the data and the information being associated with each other in separate areas.

[0019]

A tenth invention (corresponding to Claim 10) is the recording and reproducing apparatus according to any one of the fifth, eighth and ninth inventions, which is characterized in that the recording means records the reproduction information in an area that a user cannot access.

[0020]

An eleventh invention (corresponding to Claim 11) is a recording medium characterized by recording the reproduction information according to any one of the fifth, eighth, ninth and tenth inventions.

[0021]

A twelfth invention (corresponding to Claim 12) is the recording and reproducing apparatus according to any one of the fifth, eighth, ninth and tenth inventions, which is characterized in that, if the reproduction information indicates that whole or a portion of the AV data has been non-reproduced in the case where the licensing information represents a prohibition of copying or a permission of copying once, the reproducing means outputs the whole or the portion of the AV data after encrypting the whole or

the portion at the time of reproducing the AV data.

[0022]

A thirteenth invention (corresponding to Claim 13) is the recording and reproducing apparatus according to any one of the fifth, eighth, ninth and tenth inventions, which is characterized in that, if the reproduction information indicates that whole or a portion of the AV data has been reproduced in the case where the licensing information represents a prohibition of copying or a permission of copying once, the reproducing means outputs the whole or the portion of the AV data after encrypting the whole or the portion of the AV data and does not output a key for decryption at the time of reproducing the AV data.

[0023]

A fourteenth invention (corresponding to Claim 14) is the recording and reproducing apparatus according to any one of fifths, eighth, ninth, tenth and twelfth inventions, which is characterized in that, if the reproduction information indicates that whole or a portion of the AV data has been reproduced in the case where the licensing information represents a prohibition of copying or a permission of copying once, the reproducing means does not output the whole or the portion of the AV data and outputs invalid data at the time of reproducing the AV data.

[0024]

A fifteenth invention (corresponding to Claim 15) is the recording and reproducing apparatus according to any one of the first to fourth inventions characterized by comprising: a time-variant key generating means for generating a series of keys each of which varies with time; a recording encrypting means for encrypting the AV data by using the keys; and a reproducing decrypting means for decrypting the encrypted AV data; wherein: the recording encrypting means encrypts the AV data sequentially by using the keys generated by the time-variant key generating means when recording the AV data in the case where the licensing information represents a prohibition of copying or a permission of copying once; the recording means records the keys and the AV data in association with each other; the reproducing means takes out the encrypted AV data and the keys and erases the recorded portion of the taken out keys when reproducing the AV data in the case where the licensing information represents a prohibition of copying or a permission of copying once; and the reproducing decrypting means decrypts the encrypted AV data by using the taken out keys.

[0025]

A sixteenth invention (corresponding to Claim 16) is the recording and reproducing apparatus according to the fifteenth invention, which is characterized in that the

reproducing means deletes recorded positional information with respect to a key in a recording medium when erasing the recording portion of the keys.

[0026]

A seventeenth invention (corresponding to Claim 17) is the recording and reproducing apparatus according to any one of the first to fourth inventions, which is characterized by comprising: a time-variant key generating means for generating a series of keys each of which varies with time; a recording encrypting means for encrypting the AV data by using the keys; and a reproducing decrypting means for decrypting the encrypted AV data; wherein: the recording encrypting means encrypts the AV data sequentially by using the keys generated by the time-variant key generating means when recording the AV data in the case where the licensing information represents a prohibition of copying or a permission of copying once; the recording means records the keys and the AV data in association with each other; the recording is performed with adding key retrieving information indicating that the keys are not retrieved yet; the reproducing means takes out the encrypted AV data and the keys and adds thereto the key retrieving information indicating that the taken out keys have been retrieved when reproducing the AV data in the case where the licensing information represents a

prohibition of copying or a permission of copying once; and the reproducing decrypting means decrypts the encrypted AV data by using the taken out keys.

[0027]

An eighteenth invention (corresponding to Claim 18) is the recording and reproducing apparatus according to the fifteenth or seventeenth invention, which is characterized in that the recording means records the keys or the key retrieving information with the keys or the information being associated with each other in a same area as that of the AV data.

[0028]

A nineteenth invention (corresponding to Claim 19) is the recording and reproducing apparatus according to the fifteenth or the seventeen invention, which is characterized in that the recording means records the keys or the key retrieving information with the keys or the information being associated with each other in separate areas from that of the AV data.

[0029]

A twentieth invention (corresponding to Claim 20) is the recording and reproducing apparatus according to any one of the fifteenth, seventeen, eighteenth and nineteenth inventions, which is characterized in that the recording means records the keys or the key retrieving information in

an area that a user cannot access.

[0030]

A twenty-first invention (corresponding to Claim 21) is the recording and reproducing apparatus according to the tenth or twenties invention, which is characterized in that the area that a user cannot access is an area that cannot be accessed via LBA (logical block address) unit, an area wherein an area that can be accessed via the LBA unit is limited, an alternating sector area, an area other than an area to be reproduced as AV data (AUX), a RAM that is added to a recording medium, a header area of an optical disk, a power calibration area, a recording management area, a lead-in area or a lead-out area.

[0031]

A twenty-second invention (corresponding to Claim 22) is a recording medium characterized by recording the key retrieving information according to the seventeenth invention.

[0032]

A twenty-third invention (corresponding to Claim 23) is a program recording medium characterized by storing a program for letting a computer execute whole or a portion of functions of elements for the recording and reproducing apparatus according to any one of the first to twenty-second inventions.

[0033]

[Mode for Carrying out the Invention]

Embodiments of the present invention will hereinafter be described with reference to the attached drawings.

[0034]

Embodiment 1

A first embodiment will be described as a start.

[0035]

In the present embodiment, a hard disk apparatus is described by way of an example of a recording and reproducing apparatus that enables a viewer to view a program at an arbitrary time after the program has been broadcasted in the case where licensing information of AV data transmitted from a broadcasting station is "copy never" that represents a prohibition of copying. In the present embodiment, such hard disk apparatus is realized by making the AV data whose licensing information is "copy never" to be recordable and making the AV data to be reproduced only once by using a reproduction information management means. Further, there will be described a case wherein reproduction information used in the present embodiment is recorded in an area different from that of a data block on a disk medium.

[0036]

Fig. 1 is a basic configuration of the hard disk apparatus according to the present invention.

[0037]

The hard disk apparatus comprises a digital I/F means 1, a stream control means 2, an LBA access means 3, a hard disk control means 4, an actuator means 5, a disk medium 6, a head 7 and a spindle motor means 8.

[0038]

The digital I/F means 1 is a means for providing connections among external AV devices such as an STB (Set Top Box; satellite broadcasting receiver), a TV monitor, a DVHS and a hard disk apparatus and performing control of the AV devices as well as transmission of AV data. IEEE standard for High performance Serial Bus mentioned in the IEEE 1394-1995 may be used as the digital I/F means, for example. The transmission of AV data of the digital I/F means 1 is performed by a transmission method called "isochronous method", wherein real-time characteristics of the data to be transmitted are secured. Examples of the data to be transmitted include an MPEG transport stream, a DV stream and the like. The control of the AV devices of the digital I/F means 1 is performed in accordance with an asynchronous transmission method called "asynchronous method". The stream control means 2 is a means for performing an access and an authentication process of a

stream. The LBA access means is an I/F means provided inside the hard disk apparatus and used for accessing to a disk medium by designating an LBA (logical block address). The hard disc control means 4 is a means for controlling the actuator means 5 as well as the spindle motor means 8 and performing signal processing for recording and reproducing with respect to the disk medium 6 via the head 7. The head 7 is a means for recording and reproducing the signal with respect to the disk medium 6. The spindle motor means 8 is a means for rotating a disk medium at a constant rate. The actuator means 5 is a means for positioning the head 7 at a desired position on the disk medium 6.

[0039]

In the present embodiment, an EMI (Encryption Mode Indicator) generated from CGMS is used as the licensing information and, therefore, the EMI will be described below.

[0040]

Before describing the EMI, a data transmission protocol of IEEE 1394, a part of which is mentioned in connection with the digital I/F means 1, will be briefly described. When AV data is viewed via a monitor, the data must be sent in synchronization periodically. Also, in the case of controlling a stop of a hard disk apparatus or the like and a start of recording, a control command must be

sent and received at an arbitrary timing asynchronously.

In the IEEE 1394, isochronous data packets are used as the former data, and asynchronous data packets are used as the latter data.

[0041]

In the data transmission, a bus license is demanded with respect to a management node in advance of the transmission to obtain the license.

[0042]

In the asynchronous transmission, a sending node ID and a receiving node ID are sent as a data packet together with the data to be transmitted. A receiving node receives the packet after confirming its ID, and then sends an acknowledge signal back to a sending node. Thus, one transaction is performed.

[0043]

In the isochronous transmission, an isochronous channel is requested together with a transmission speed at the side of the receiving node. A channel ID is sent as a data packet together with the data to be transmitted. The receiving node receives the packet after confirming the desired channel ID.

[0044]

The above is the brief description of the data transmission protocol of the IEEE 1394.

[0045]

Now, description returns to the EMI. The CGMS is added to the AV data at a broadcasting station. The STB that receives a broadcast wave sent from the broadcasting station sends the received program to the IEEE 1394 bus. In this case, the CGMS is embedded in a portion of service information of the MPEG transport stream of the isochronous data packets. A plurality of pieces of MPEG data are stored in one isochronous data packet, and each set of the MPEG data is provided with a corresponding CGMS.

[0046]

The EMI comprises such CGMS and is generated by the STB. The STB investigates the CGMS of each of the AV data to be transmitted as an isochronous data packet and apply one EMI to one isochronous data packet as a representative value. The EMI is retained at a header portion of the isochronous data packet.

[0047]

The CGMS takes the following value. Namely, "CGMS = 11" represents a prohibition of copying (copy never); "CGMS = 10" represents a permission of copying only for one generation (copy one generation); and "CGMS = 00" represents a liberty of copying (copy free).

[0048]

A value that the EMI takes is a value of CGMS that

is the most strict in limitation of licensing conditions among CGMS of AV data existing in one isochronous data packet. For example, when CGMS of AV data in one isochronous data packet are 11, 10 and 10, the value of the EMI is 11 that represents the most strict limitation among them. Also, in the case where the CGMS are 10, 10, 00 and 00, the value of the EMI is 10 that represents the most strict limitation among them. The value of the EMI is determined in the above manner.

[0049]

Values taken by the EMI are "EMI = 11" representing a prohibition of copying (copy never); "EMI = 10" representing a permission of copying only for one generation (copy one generation); and "EMI = 00" representing a liberty of copying (copy free). The above is the same as the case of the CGMS. A value taken only by the EMI is "EMI = 01" that represents a change of the EMI after recording AV data of copy one generation and prohibits any more copying (no more copy).

[0050]

The above is the description of the EMI.

[0051]

Referring back to Fig. 1, the stream control means 2 of the hard disk apparatus is configured as shown in Fig. 2. Namely, the stream control means 2 comprises an EMI

detecting means 9, an EMI applying means 10, an EMI access means 11, an EMI judging means 12, an authenticating and encrypting means 13, an invalid data outputting means 14, a file access means 15, a stream access means 16, a reproduction information managing means A17, a data block access means 18 and a selecting switch 19.

[0052]

The EMI detecting means 9 is a means for detecting a field wherein an EMI is written in from a header portion of an isochronous data packet inputted from the digital I/F means 1. The EMI applying means 10 is a means for applying a designated EMI to a header portion of an isochronous data packet to be outputted to the digital I/F means 1. The EMI access means 11 is a means for reading out the detected EMI information via the LBA access means 3 and recording and reproducing the detected EMI information in association with a designated data block. The EMI judging means 12 is a means for judging a presence or absence of a license as well as a type of the license from the EMI information. The authenticating and encrypting means 13 is a means for performing authentication among the AV devices via the digital I/F means 1, decryption of AV data inputted from the digital I/F means 1 and encryption of the AV data read out from the disk medium 6 via the data block access means 18. The data block access means 18 is a means for

recording or reproducing data having a designated block number via the LBA access means 3 and informing the EMI access means 11 and the reproduction information managing means A17 of which block number is currently accessed. The stream access means 16 is a means for designating a block number to be recorded or reproduced to the data block access means 18 in order to execute a command of the access method 2 received from the digital I/F means 1, performing a stream pointer management to indicate a current block position of a stream in accordance with instructions of reproduction, recording, stop and the like with assuming a first data block to a last data block of a user area as a rope, and recording or reading out stream pointer management information with respect to the disk medium 6 via the LBA access means 3. Here, the access method 2 is a method according to, for example, AV/C Digital Interface Command Set VCR subunit Specification version 2.0.1. The file access means 15 is a means for designating a block number to be recorded or reproduced to the data block access means 18 in order to execute a command of the access method 3 received from the digital I/F means 1; having file management information; managing file names and order structures of a plurality of data blocks constituting each of the files; managing a file pointer indicating a block position in a file that is currently processed in

accordance with instructions of reproduction, record, stop and the like of the command of the access method 3; and recording or reading out the order structure information of data block of the files, file pointer information and the like with respect to the disk medium 6 via the LBA access means 3. Here, the access method 3 is an access method for controlling an AV apparatus by designating a file name and process contents of the file, reproduction, recording, stop and the like in accordance with, for example, AV/C Digital Interface Command Set General Specification. The selecting switch 19 is a means for outputting invalid data such as a blue back or a black screen by switching off or switching to the invalid data outputting means in the case where the data has been reproduced based on the results of the reproduction information management means A17 when the AV data is output to the digital I/F means 1 via the EMI applying means 10, and outputting the encrypted AV data by switching to the authenticating and encrypting means 13 in the case of non-reproduction. The reproduction information management means A17 is a means for recording and reading out reproduction information corresponding to a designated data block as well as for judging if the data has been reproduced or not from the reproduction information.

[0053]

The authenticating and encrypting means 13 of Fig. 2

is configured as shown in Fig. 3. Namely, it comprises a decrypting means 20, an authenticating means 21, a key generating means 22, an encrypting means 23, a selecting switch 24 and a selecting switch 25.

[0054]

The authenticating means 21 is a means for performing authentications among the AV apparatuses that provide connections among the digital I/F means 1; and, when the authentications are successful, sending a key that the authenticating means 21 used for encryption to other devices in the case where AV data is to be outputted to the side of the digital I/F means 1 as well as receiving a key that the authenticating means 21 will use for decryption from other devices in the case where AV data is to be inputted from the side of the digital I/F means 1. The encrypting means 23 is a means for encrypting the AV data read out from the disk medium via the data block access means by using a key generated by the key generating means 22 to output the encrypted AV data to the digital I/F means 1. The key generating means 22 is a means for generating the key used for the encryption and sending the key to the encrypting means 23 as well as to the authenticating means 21. The decrypting means 20 is a means for decrypting the encrypted AV data that is inputted from the digital I/F means 1 by using the key obtained by the authenticating

means 21 to output the decrypted AV data to the data block access means 18. The switches 24 and 25 are a means for switching in such a manner that inputted and outputted data do not go through the encrypting means 23 and the decrypting means 20 when EMI is 00 with respect to the judgment results of the EMI judging means 12 and that inputted and outputted data go through the encrypting means 23 and the decrypting means 20 when the EMI is other than 00.

[0055]

The reproduction information managing means A17 of Fig. 2 is configured as shown in Fig. 4. It comprises a reproduction information updating means 26, a reproduction judging means 27, a reproduction information generating means 28, a reproduction information access means 29 and a selecting switch 30.

[0056]

The reproduction information generating means 28 is a means for generating reproduction information that initializes a reproduction flag "play_flag" by 0, for example. The corresponding AV data is regarded to be not reproduced when the "play_flag" is 0. The reproduction information updating means 26 is a means for updating the reproduction information to be information indicating that the data is already reproduced. For example, the

reproduction information updating means 26 updates a reproduction flag "play_flag" by 1. The corresponding AV data is regarded to be already reproduced when the "play_flag" is 1. The reproduction information access means 29 is a means for storing reproduction information corresponding to each of the data blocks as a table and recording or reading out the reproduction information with respect to the disk medium 6 via the LBA access means 3. The reproduction judging means 27 is a means for judging whether or not AV data has been reproduced based on the reproduction information read out by the reproduction access means 29. For example, the reproduction judging means 27 judges that the AV data has been reproduced once if the reproduction flag "play_flag" is 1 and, also, updates the reproduction information (reproduction flag) by using the switch 30 if it is judged that the AV data has been non-reproduced in the case where the EMI is 11 (copy never) based on the EMI judging results. The switch 30 is a means for switching to the side of the reproduction information generating means 28 if the reproduction judging means 27 judges that new AV data is to be recorded and switching to the side of the reproduction updating means 26 if it is judged that the AV data has been recorded at the time of reproduction or the like.

[0057]

The operation of the present embodiment will be described below.

[0058]

The STB is considered as a device that sends AV data. Further, there is a controller for sending a program receiving command, recording start command, recording stop command or like commands to the IEEE 1394 bus; however, a description of sending and receiving commands between the controller and the hard disk apparatus as well as between the controller and the STB is omitted in this specification since such description will be a deviation from the subject matter of the present embodiment.

[0059]

There will be described a case wherein the controller sends a receiving start command for starting to receive a program transmitted from a broadcasting station to the STB and sends a recording start command to the hard disk apparatus as a start. A case wherein AV data is sent from apparatus other than the STB such as a DVHS, a hard disk apparatus and like recording and reproducing apparatuses will be described later in this specification. The program transmitted from the broadcasting station is received by the STB and then an EMI is applied thereto to be sent to the IEEE 1394 bus as an isochronous data packet. The hard disk apparatus receives the recording start

command in accordance with the command of the access method 2 or 3 from the digital I/F means 1, and then the digital I/F means 1 confirms a desired channel number to fetch a corresponding isochronous data packet. If the recording start command is received in accordance with the command of the access method 2, the authentication means 21 sends an authenticating command to the STB. The EMI detecting means 9 detects EMI information retained at a header portion of the fetched isochronous data packet. The EMI judging means 12 judges a presence or absence of a license and a type thereof from the detected EMI information. Results of the judgment is inputted to the authenticating and encrypting means 13, and the authenticating means 21 decides an authenticating method depending on the presence or absence of license and the type thereof. If the EMI is 11, i.e., in the case of "copy never", a public key will be used for the authentication since the AV data is highly important. If the EMI is 10, i.e., in the case of "copy one generation", a common key is used for the authentication since the AV data is less important than the case where the EMI is 11. If the EMI is 00, i.e., in the case of "copy free", no authentication is actually performed since the AV data is not important and it is regarded that the authentication is successfully performed. The STB receives an authentication command and performs an authentication by

using the public key or the common key with respect to the hard disk apparatus. If the authentication is successful, the relevant key is sent to the hard disk apparatus. The authenticating means 21 receives the key sent from the STB via the digital I/F means 1, and then sends the received key to the decrypting means 20. Note that the authenticating means 21 does not receive the key from the STB in the case where the EMI is 00. In such cases, the AV data is not encrypted. The decrypting means 20 receives the key from the authenticating means 21 when the EMI is 11 and when the EMI is 10. It is assumed that a record command is received via the digital I/F means 1 in accordance with the command of the access method 2. Succeeding process will be described with reference to a flowchart of Fig. 10. In the case where an EMI of AV data is not 00, the selecting switch 24 is so switched via the digital I/F means 1 that the AV data goes through the decrypting means 20. Also, in the case where an EMI is 00, the selecting switch 24 is so switched that the AV data does not go through the decrypting means 20. The decrypting means 20 decrypts the AV data that has been encrypted by using a key received thereby. The stream access means 16 instructs the data block access means 18 to record a block x. The data block access means 18 informs the EMI access means 11 of a block number (= x) that is

currently accessed. The EMI accessing means 11 records EMI information detected by the EMI detecting means 9 with the EMI information being associated with the informed block number. Note that, in the case where the EMI is 10, i.e., "copy one generation", the EMI access means 11 records the EMI information on the disk medium 6 with the EMI being rewritten to 01, i.e., "no more copy". The data block access means 18 informs the reproduction information managing means A17 of the block number ($= x$) that is currently accessed. The selecting switch 30 is switched to the side of the reproduction information generating means 28 in the case of recording. The reproduction information access means 29 records the reproduction information as a table with the reproduction information being associated with the block number ($= x$). The reproduction information generating means 28 registers information indicating that the AV data is non-reproduced to the reproduction information. That is to say, the reproduction information generating means 28 initializes the reproduction information by "play_flag = 0" (S1). The reproduction information access means 29 records the reproduction information on the disk medium 6 via the LBA access means 3 (S2). Next, the block number is incremented by one. That is to say, the block number is set to be $x = x + 1$ (S3). It is then judged whether or not another command is

received from the digital I/F means 1 (S4). In the case where another command has been received, the process is brought to an end. In the case where another command has not been received, the process after receiving the record command is repeated until another command is received. The above is the description of the case of recording AV data on the disk medium 6.

[0060]

A case wherein a hard disk apparatus reproduces AV data will be described below. The case of reproducing the AV data on a TV monitor is considered. Further, it is assumed that the AV data recorded in the hard disk apparatus is recorded from an STB. Note that there exists a controller for sending a reproduction start command, reproduction stop command and the like to an apparatus connected via the IEEE 1394 bus; however, description of sending and receiving of the commands between the controller and the hard disk apparatus as well as between the controller and the TV monitor is omitted in the present embodiment since such description will be a deviation from the subject matter of the present embodiment.

[0061]

The controller sends the reproduction start command to the TV monitor and the hard disk apparatus. The data block access means 18 of the hard disk apparatus informs

the reproduction information management means A17 and the EMI access means 11 of an access point. The EMI access means 11 takes out EMI information of the informed access point and sends the EMI information to the EMI applying means 10. The selecting switch 19 is switched to the side of invalid data outputting means 14, and invalid data such as a blue back screen and a black screen is sent to the EMI applying means 10. The EMI applying means 10 sends the EMI information sent from the EMI access means 11 and the AV data sent from the invalid data outputting means 14 as an isochronous data packet to the IEEE 1394 bus via the digital I/F means 1. The TV monitor sends an authentication command to the hard disk apparatus. The TV monitor fetches the isochronous data packet sent from the hard disk apparatus and decides an authentication method with reference to the EMI information applied to the isochronous packet data. In the case where the EMI is 11, i.e., "copy never", the authenticating means 21 performs an authentication with the TV monitor using the public key via the digital I/F means 1. In the case where the EMI is 01, i.e., "no more copy", the authenticating means 21 performs an authentication with the TV monitor using the common key via the digital I/F means 1. In the case where the EMI is 00, no authentication is actually performed and it is regarded that an authentication is successfully performed.

The AV data wherein the EMI is 10, i.e., "copy one generation" is recorded after the EMI is rewritten to be 01 since the case of reproducing the AV data sent from the STB is treated in the present embodiment. When the hard disk apparatus receives the authentication command via the digital I/F means 1, the authenticating means 21 decides a type of the authentication with reference to the EMI information and then performs an authentication with the TV monitor. If the authentication is successful, the authenticating means 21 sends a key generated by the key generating means 22 to the encrypting means 23. In the case where the EMI is 00, the key is not sent to the encrypting means 23, and the selecting switch 25 is so switched that the AV data does not go through the encrypting means 23. The selecting switch 19 is switched to the side of the authenticating and encrypting means 13.

[0062]

Succeeding operation can be performed by either one of two types of operations depending on when the reproduction information is updated by the reproduction information management means A17. A first case is a case wherein the reproduction information is updated at a time after finishing the reproduction, and a second case is a case wherein the reproduction information is updated per block during reproduction.

[0063]

The first case will be described with reference to the flowchart of Fig. 10.

[0064]

It is assumed that the hard disk apparatus receives a reproduction command in accordance with the command of the access method 2 from the digital I/F means 1. The stream access means 16 instructs the data block access means 18 to reproduce a block x. The data block access means 18 informs the EMI access means 11 and the reproduction information managing means A17 of a block number (= x) that is currently accessed. At the same time, the data block access means 18 reads out AV data from the disk medium 6 via the LBA access means 3 (S5). The EMI access means 11 reads out EMI information corresponding to the informed block number from the disk medium 6. The read out EMI information is judged by the EMI judging means 12, and the judgment results are sent to the authenticating and encrypting means 13 as well as to the reproduction judging means 27.

[0065]

In the case where the EMI is 00 in the EMI judging results (S6), the selecting switch 25 is switched to the side where the AV data does not go through the encrypting means 23 so that the AV data is outputted without being

encrypted (S8). In the case where the EMI is not 00 (S6), the selecting switch is switched to the side where the AV data goes through the encrypting means 23. The selecting switch 30 is switched to the side of the reproduction information updating means 26 at the time of reproduction. The reproduction judging means 27 examines the judgment results of the read out EMI information.

[0066]

In the case where the EMI is 11, the reproduction judging means 27 judges whether the AV data has been non-reproduced or reproduced (S7). In the case where the EMI is 11 (copy never) and the AV data has been reproduced, the selecting switch 19 is switched to the side of the invalid data outputting means 14 to output invalid data such as a blue back screen or a black screen (S10). In the case where the EMI is 11 (copy never) and the AV data has been non-reproduced or in the case where the EMI is not 11, the selecting switch 19 is switched to the side of the authenticating and encrypting means 13 so that the AV data is encrypted by the encrypting means 23 to be outputted via the digital I/F means 1 (S8).

[0067]

Next, the block number is incremented by one. That is to say, the block number is set to be $x = x + 1$ (S9). It is then judged if another command has been received from

the digital I/F means 1 (S11). If another command has been received, the process is brought to an end. When the reproduction process is completed, the reproduction information containing numbers of the reproduced blocks from an initial value number to a last value number reproduced by the reproduction information access means 29 is accessed so that the reproduction information updating means 26 updates the reproduction information reproduced, i.e., "play_flag = 1" (S12). In the case where another command is not received, the process after receiving the reproduction command is repeated until another command is received. The above is the description of the case of reproducing the AV data according to the first case.

[0068]

The second case will be described with reference to the flowchart of Fig. 11 below.

[0069]

It is assumed that the hard disk apparatus receives a reproduction command in accordance with the command of the access method 2 from the digital I/F means 1. The stream access means 16 instructs the data block access means 18 to reproduce a block x. The data block access means 18 informs the EMI access means 11 and the reproduction information managing means A17 of a block number (= x) that is currently accessed. At the same time

the data block access means 18 reads out the AV data from the disk medium 6 via the LBA access means 3 (S17). The EMI access means 11 reads out EMI information corresponding to the informed block number from the disk medium 6. The read out EMI information is judged by the EMI judging means 12, and the judgment results are sent to the authenticating and encrypting means 13 and the reproduction judging means 27.

[0070]

In the case where the EMI is 00 in the EMI judgment results (S18), the selecting switch 25 is switched to the side where the AV data does not go through the encrypting means 23, so that the AV data goes through the authenticating and encrypting means 13 as well as the digital I/F means 1 to be outputted without being encrypted (S21). In the case where the EMI is not 00 (S18), the selecting switch 25 is switched to the side where the AV data goes through the encrypting means 23. The selecting switch 30 is switched to the side of the reproduction information updating means 26 at the time of reproduction. The reproduction judging means 27 examines the judgment results of the read out EMI information.

[0071]

In the case where the EMI is not 00, it is judged whether the AV data has been non-reproduced or reproduced

(S19). In the case where the EMI is 11 (copy never) and the AV data has been reproduced (play_flag = 1), the selecting switch 19 is switched to the side of the invalid data outputting means 14 so that invalid data such as a blue back screen and a black screen are outputted (S22). When it is judged by the reproduction judging means 27 that the EMI is 11 (copy never) and the AV data has been non-reproduced (play_flag = 0), the reproduction information updating means 26 updates the reproduction information to indicate that the data has been reproduced, i.e., "play_flag = 1" (S20). Then, the selecting switch is switched to the side of the authenticating and encrypting means 13, so that the AV data read out by the data block access means 18 is encrypted by the encrypting means 23, and then is outputted via the digital I/F means 1 (S21). The reproduction information of the block x is updated by the reproduction information access means 29 (S23). The block x is set to be x + 1 (S24), and the process is brought to an end when a command other than the reproduction command is received (S25). In the case where the command other than the reproduction command is not received, the process after receiving the reproduction command is repeated until another command is received.

[0072]

The above is the description of reproducing AV data

in accordance with the second case.

[0073]

In the case where the EMI of AV data recorded in the hard disk is 11 (copy never), it is possible to reproduce once the AV data of "copy never" by switching the selecting switch depending on the judgment made by the reproduction information managing means A17 and managing the reproduction information by the reproduction information managing means A17.

[0074]

In addition, a case of executing a command by using the stream access means 16 in accordance with the access method 2 has been described in the present embodiment; however, the invention is not limited thereto and it is possible to execute the command by using the file access means 15 in accordance with the access method 3. In this case, the order of recording and reproducing does not depend on the order of the block numbers, but depends on the order of blocks managed by the file management information. That is to say, if an x-th block to be recorded and reproduced is $f(x)$, the block x shown in Figs. 10 and 11 has only to be replaced by the block $f(x)$.

[0075]

It is also possible to select and execute a method of authentication corresponding to an EMI. Namely, 2 types

of authentication methods may be employed. Authentication method A is used as an authentication method for the case wherein the EMI is 11 (copy never). Authentication method B is used as an authentication method for the case wherein the EMI is 10 (copy one generation) and the case wherein the EMI is 01 (no more copy). An authentication using a public key is employed as the authentication method A, and an authentication using a common key is employed as the authentication method B. The devices that do not record the AV data such as the TV monitor and the STB support both of the methods A and B, and the devices that record the AV data such as VTR support only the method B. Further, the hard disk apparatus of the present invention supports both of the authentication methods A and B. It is assumed that the hard disk apparatus of the present invention records AV data sent from the STB. The hard disk apparatus and the STB support both of the authentication methods A and B; therefore, the authentication is successful when the EMI is not 00 so that the AV data is recorded in the hard disk apparatus of the present invention. In the case where the AV data is reproduced on a TV monitor at the time of reproduction of the hard disk apparatus of the present invention, the authentication is successful if the EMI is 11 (copy never) since the TV monitor supports the authentication method A, so that the AV data can be

outputted on the TV monitor. The license of "copy never" can be honored since the TV monitor does not record the AV data. Also, in the case where the EMI is 10 (copy one generation) or the EMI is 01 (no more copy), the authentication is successful since the TV monitor supports the authentication method B, so that the AV data can be outputted on the TV monitor. In turn, in the case where AV data wherein an EMI is 11 (copy never) is outputted to a VTR, the hard disk apparatus of the present invention tries to perform the authentication method A. But the VTR does not support authentication other than the authentication method B and, therefore, the authentication fails to succeed. Thus, the AV data wherein the EMI is 11 cannot be recorded in the VTR. In turn, in the case where the EMI is 10 (copy one generation) or 01 (no more copy), the authentication method B is employed. The authentication is successful since the VTR supports the authentication method B. In the case where the EMI is 10 (copy one generation), the AV data can be recorded in the VTR. In the case where the EMI is 01 (no more copy), the authentication is successful, while the AV data is not recorded since the VTR is prohibited to record the AV data of "no more copy". Further, there may be considered a case wherein 2 sets of the hard disk apparatus of the present invention are used and one of them (hereinafter referred to as disk apparatus

A) outputs AV data wherein an EMI is 11 (copy never) and the other (hereinafter referred to as disk apparatus B) records the AV data. In this case, the disk apparatuses A and B perform an authentication in accordance with the authentication method A to each other, and the AV data can be transmitted from the disk apparatus A to the disk apparatus B. Here, the disk apparatus A outputs the AV data only once and, therefore, the disk apparatus A cannot output the AV data any more. As a result, the AV data is transferred from the disk apparatus A to the disk apparatus B. However, the receiving end of the data is not the TV monitor and, therefore, a user cannot view the AV data during the transfer. In other words, the AV data can be transferred. Thus, it is possible to honor the license easily.

[0076]

Further, as mentioned above, there will be described a case wherein AV data sent from a device other than the STB is recorded in the hardware apparatus of the present invention. The AV data sent from the STB does not include the data wherein an EMI is 01 (no more copy). However, in the case where AV data is sent from a device other than the STB, the AV data includes those wherein the EMI is "no more copy". In the case where the EMI is 01 (no more copy), the data access means 18 and the EMI access means 11 serve to

prohibit the AV data and EMI information from being recorded on the disk medium 6. Other operations are the same as those of the case of recording the AV data sent from the STB. In the case of performing reproduction and recording between hard disk apparatuses of the present invention, it is possible to transfer the AV data having the EMI of 11 (copy never) from one of the apparatuses that serves for reproduction to the other one of the apparatuses that serves for recording.

[0077]

In the case where the EMI is other than 11, the same operations as those of connecting the hard disk apparatus of the present invention to the VTR will be performed. It is thus possible to authenticate highly important AV data such as "copy never" by employing a safer method such as the public key as a result of selecting an authentication method corresponding to an EMI.

[0078]

Here, following 2 cases will be described by way of example for storing reproduction information and AV data to a disk medium.

[0079]

A case wherein the reproduction information is retained by block unit will be described at first. In Fig. 5, the disk medium 6 is divided into a system area 31 and a

user area 32. The system area 31 is an area to be used by the system but a user cannot access. In turn, the user area 32 is an area used by the user. The user area 32 is constituted of k blocks. A reproduction information recording section 33 is provided at a part of the system area 31. The reproduction information for each of the k blocks is recorded in the reproduction information recording section 33. A first block (34), a second block (35), a third block (36) and a k-th block (37) of the reproduction information are represented by 0 in a table stored in a bit map form in the reproduction information recording section (33). This represents that the blocks are non-reproduced areas. Note that the area such as k-th block (37) is an area that is not used yet and, thus, free area is also represented by 0 in terms of the reproduction information. Further, since the reproduction information of an eleventh block, a twelfth block and a thirteenth block is represented by 1, the blocks are reproduced areas. Such reproduction information recording section 31 is created and updated by the reproduction information managing means A17. The user cannot tamper contents of the reproduction information recording section 33 to view AV data illegally since the reproduction information recording section 33 is stored in the system area 31. Thus, reliability of a hard disk having a function of the present

embodiment is improved.

[0080]

A case wherein reproduction information is managed by using addresses is described below. Referring to Fig. 6, the disk medium 6 is divided into a system area 38 and a user area 39. The system area 38 is an area to be used by the system but a user cannot access. In turn, the user area 39 is used by the user. Stream is defined by dividing data every time the reproduction information changes from reproduced to non-reproduced or from non-reproduced to reproduced. A reproduction information recording section 40 represents the reproduction information by using reproduction information of the stream and a start LBA and an end LBA of the stream. A first stream (41) has a start LBA of 0 and an end LBA of a1, and all the LBA of this stream have been non-reproduced. A second stream (42) has a start LBA of a1 and an end LBA of a2, and this stream has been reproduced. A third stream (43) has a start LBA of a2 and an end LBA of a3, and this stream has been non-reproduced. An n-th stream has a start LBA of a4 and an end LBA of a5, and reproduction information of this stream has been reproduced. Such reproduction information recording section 40 is created and updated by the reproduction information managing means A17. A user cannot tamper contents of the reproduction information recording

section 33 to view AV data illegally since the reproduction information recording section 40 is stored in the system area 38. Thus, reliability of a hard disk having a function of the present embodiment is improved.

[0081]

The reproduction information recording section 33 or 40 may not necessarily be provided at the system area 31 or 38, and may be provided in an alternating sector area in a hard disk apparatus.

[0082]

It is possible to realize above described embodiment by using an optical disk apparatus (such as DVD-RAM) in place of the hard disk apparatus. In this case, the reproduction information recording section 33 or 40 may be provided as an area that cannot be accessed by a user illegally such as a so-called power calibration area (PCA) for proof writing used for adjusting laser power in the case of the DVD-R shown in Fig. 24 or a so-called recording management area (RMA) for recording positional information to be added and so on in the case of additionally writing data. Further, The reproduction information recording section 33 or 40 may be a lead-in area wherein TOC information and so on are recorded or a read-out area that represents an end. As shown in Fig. 25, in the case of using the DVD-RAM, the reproduction information recording

section 33 or 40 may be a header portion wherein ID information of each sectors is recorded in addition to the above areas. In the DVD-RAM, data can be recorded in the alternating sector area. In other words, the reproduction information may be recorded in any area irrelevant to a mode of recording medium as long as the user cannot change data directly.

[0083]

The EMI information is recorded and reproduced with respect to the disk medium 6 via the LBA access means by the EMI access means 11; however, it is possible to prohibit the user from tampering the EMI information and viewing the EMI information illegally by recording the EMI information in the system area of the disk medium 6 or the like where the user cannot change data directly in the same manner as in the reproduction information. Thus, reliability of the hard disk apparatus having a function of the present embodiment is improved.

[0084]

Embodiment 2

A second embodiment will be described below.

[0085]

In the present embodiment, a hard disk apparatus is described by way of an example of a recording and reproducing apparatus that enable a viewer to view a

program at an arbitrary time after the program has been broadcasted in the case where licensing information of AV data transmitted from a broadcasting station is "copy never" that represents a prohibition of copying.

[0086]

In the present embodiment, such hard disk apparatus is realized by making the AV data whose licensing information is "copy never" to be recordable and making the AV data to be reproduced only once by using a reproduction information management means.

[0087]

Although the reproduction information and the data blocks are recorded respectively in separate areas in the first embodiment, the reproduction information and the data blocks are recorded in an identical area in the present embodiment.

[0088]

The configuration of the embodiment 2 will be described below in terms of points that are different from the first embodiment.

[0089]

Referring to Fig. 7, a reproduction information managing means B45 is a means for reading out and updating reproduction information associated with a designated data block and judging from the reproduction information whether

or not the data has been reproduced. A reproduction information generating and EMI mixing means 46 is a means for pairing EMI information and reproduction information with a data block and initializing the reproduction information so that it represent a state of non-reproduction. A reproduction information EMI separating means 47 is a means for separating and extracting the EMI information and the reproduction information paired from the data block.

[0090]

The reproduction information managing means B45 is configured as follows. Namely, the reproduction information managing means B45 comprises a reproduction information updating means 26, a reproduction judging means 27, a reproduction information access means 29 and a selecting switch 48.

[0091]

The reproduction information updating means 26 is a means for updating the reproduction information so that the information represents that AV data has been reproduced. For example, it is a means for performing updates by using a reproduction flag "play_flag = 1". The reproduction information access means 29 is a means for updating the reproduction information corresponding to each of the data blocks; recording data in the disk medium 6 via the LBA

access means 3; storing the reproduction information corresponding to each of the data blocks as a table; and having a function of cache. The reproduction judging means 27 is a means for judging whether or not the AV data is reproduced based on the reproduction information read out by the reproduction information access means 29. For example, the reproduction judging means 27 judges that the AV data has been reproduced once if the reproduction flag is "play_flag = 1" and judges that the AV data has been non-reproduced if "EMI = 11" based on EMI judgment results. If it is judged that the AV data has been non-reproduced, the reproduction judging means 27 lets the selecting switch 48 switch to the side of the reproduction information updating means 26 and updates the reproduction information. Also, the reproduction judging means 27 is a means for switching off the selecting switch 19 or switching the selecting switch 19 to the invalid data outputting means 14 if it is judged that the AV data has been reproduced when "EMI = 11".

[0092]

Operations of the present embodiment will be described below.

[0093]

In the present embodiment, AV data sent from an STB is recorded and reproduced by a hard disk apparatus in the

same manner as the first embodiment. Descriptions of authentication and exchange of keys between the STB and the hard disk apparatus of the present embodiment are omitted since they are the same as those of the first embodiment.

[0094]

Now, it is assumed that a record command is received via the digital I/F means 1 in accordance with the command of the access method 2. Succeeding process will be described with reference to the flowchart of Fig. 10. In the case where an EMI of the AV data is not 00, the selecting switch 24 is switched so that the AV data goes through the decrypting means 20. In the case where the EMI is 00, the selecting switch 24 is switched so that the AV data does not go through the decrypting means 20. The decrypting means 20 decrypts the encrypted AV data by using a key that is received thereby. The stream access means 16 instructs the data block access means 18 to record a block x. The data block access means 18 informs the reproduction information managing means B45 of a block number (= x) that is currently accessed. The EMI is detected by the EMI detecting means 9 and then judged on a presence or absence of a license and a type thereof by the EMI judging means 12. The judgment results are sent to the reproduction information generating and EMI mixing means 46. The reproduction information generating and EMI mixing means 46

pairs the EMI information and the reproduction information with the data block and initializes the reproduction information to represent a state of non-reproduction. Namely, a reproduction flag of the reproduction information is set to be "play_flag = 0". Note that in the case where the EMI is 10 (copy one generation), the EMI is rewritten to 01 (no more copy). The reproduction information generating and EMI mixing means 46 sends data which is made by pairing the AV data, the reproduction information and the EMI information to the data block access means 18. The block access means 18 stores the paired data in the block x of the disk medium 6 via the LBA access means 8 (S2). A format to be stored in the block x will be described later in this specification. Then, the block number is incremented by one, i.e., the block number is set to be $x = x + 1$ (S3). Next, it is judged if another command is received from the digital I/F means 1 (S4). In the case where another command has been received, the process is brought to an end. In the case no other command has been received, the process after receiving the record command is repeated until another command is received. The above is the description of recording AV data on the disk medium 6.

[0095]

There will be described a case wherein a hard disk apparatus reproduces AV data. A case wherein the AV data

is reproduced on a TV monitor is considered. Further, it is assumed that the AV data recorded in the hard disk is recorded from the STB. Descriptions of authentication and exchange of keys between the TV monitor and the hard disk apparatus of the present embodiment are omitted since they are the same as those of the first embodiment.

[0096]

Two types of operations can be performed depending on when the reproduction information managing means B45 updates the reproduction information. A first case is a case wherein the reproduction information is updated at a time after the reproduction is completed, and a second case is a case wherein the reproduction information is updated per block during reproduction.

[0097]

The first case will be described with reference to the flowchart of Fig. 10.

[0098]

It is assumed that the hard disk apparatus receives a reproduction command in accordance with the command of the access method 2 from the digital I/F means 1. The stream access means 16 instructs the data block access means 18 to reproduce a block x. The data block access means 18 informs the reproduction information managing means B45 of a block number (= x) that is currently

accessed. At the same time, the data block access means 18 reads out AV data wherein the EMI information is paired with the reproduction information from the disk medium 6 via the LBA access means 3 (S5). The reproduction information and EMI separating means 47 separates the EMI information and the reproduction information from the paired data. The EMI information is sent to the EMI applying means 10 as well as to the EMI judging means 12, and the reproduction information is sent to the reproduction judging means 27. The EMI judging means 12 judges the EMI information, and the judgment results are sent to the authenticating and encrypting means 13 as well as to the reproduction judging means 27.

[0099]

In the case where the EMI is 00 in the EMI judgment results (S6), the selecting switch 25 is switched to the side that the AV data does not go through the encrypting means 23, so that the AV data is outputted without being encrypted (S8). In the case where the EMI is not 00 (S6), the selecting switch 25 is switched to the side that the AV data goes through the encrypting means 23. The selecting switch 48 is switched to the side of reproduction information updating means 26 at the time of reproduction only in the case where "EMI = 11". The reproduction judging means 27 examines the judgment results of the read

out EMI information.

[0100]

In the case where the EMI is 11 (copy never), the reproduction judging means 27 judges whether the AV data has been non-reproduced or reproduced (S7). In the case where the EMI is 11 (copy never) and the AV data has been reproduced, the selecting switch 19 is switched to the side of the invalid data outputting means 14 to output invalid data such as a blue back screen or a black screen (S10). In the case where the EMI is 11 (copy never) and the AV data has been non-reproduced or in the case where the EMI is not 11, the selecting switch 19 is switched to the side of the authenticating and encrypting means 13 so that the AV data is encrypted by the encrypting means 23 and then outputted via the digital I/F means 1 (S8).

[0101]

Then, the block number is incremented by one, i.e., the block number is set to be $x = x + 1$ (S9). Next, it is judged if another command has been received from the digital I/F means 1 (S11). If another command has been received, the process is brought to an end. When the reproduction process is completed, the reproduction information containing the reproduced blocks of the initial value number to the last value number is accessed by the reproduction information access means 29, and then updated

to have been reproduced, i.e., to be "play_flag = 1" by the reproduction information updating means 26 (S12). In the case where no other command has been received, the process after receiving the reproduction command is repeated until another command is received. The above is the case of reproducing the AV data in accordance with the first case.

[0102]

The second case will be described below with reference to the flowchart of Fig. 11.

[0103]

It is assumed that the hard disk apparatus receives a reproduction command in accordance with the command of the access method 2 from the digital I/F means 1. The stream access means 16 instructs the data block access means 18 to reproduce a block x. The data block access means 18 informs the reproduction information access means 29 of a block number (= x) that is currently accessed. At the same time, the data block access means 18 reads out AV data wherein EMI information is paired with reproduction information from the disk medium 6 via the LBA access means 3. The reproduction information and EMI separating means 47 separates the EMI information and the reproduction information from the AV data. The EMI information is sent to the EMI applying means 10 as well as to the EMI judging means 12, and the reproduction information is sent to the

reproduction judging means 27. The EMI judging means 12 judges the EMI information, and the judgment results are sent to the authenticating and encrypting means 13 as well as to the reproduction judging means 27.

[0104]

In the case where the EMI is 00 in the judgment results (S18), the selecting switch 25 is switched to the side that the AV data does not go through the encrypting means 23, so that the AV data is given the EMI information at the EMI applying means 10 without going through the authenticating and encrypting means 13 and then outputted via the digital I/F means 1 without being encrypted (S21). In the case where the EMI is not 00 (S18), the selecting switch 25 is switched to the side that the AV data goes through the encrypting means 23. The selecting switch 30 is switched to the side of the reproduction information updating means 26 at the time of reproduction. The reproduction judging means 27 examines the judgment results of the read out EMI information.

[0105]

In the case where the EMI is 11 (copy never), it is judged if the AV data has been non-reproduced or reproduced (S19). In the case where the EMI is 11 (copy never) and the AV data has been reproduced, i.e., "play_flag = 1", the selecting switch 19 is switched to the side of the invalid

data outputting means 14 to output invalid data such as a blue back screen and a black screen (S22). In the case where the reproduction judging means 27 judges that the EMI is 11 (copy never) and the data has been non-reproduced, i.e., "play_flag = 0", the reproduction information updating means 26 updates the reproduction information to have been reproduced, i.e., to be "play_flag = 1" (S20). Then, the selecting switch 19 is switched to the side of the authenticating and encrypting means 13, so that the AV data read out by the data block access means 18 is encrypted by the encrypting means 23 to be outputted via the digital I/F means 1 after being given an EMI by the EMI applying means 10 (S21). Further, the reproduction information access means 29 updates the reproduction information of the block x (S23). The block x is set to be $x + 1$ (S24), and the process is brought to an end when a command other than a reproduction command is received (S25). In the case where no command is received, the process after receiving the reproduction command is repeated until another command is received. The above is the case of reproducing AV data in accordance with the second case.

[0106]

As mentioned above, there will be described a format of data that are generated by the reproduction information generating and EMI mixing means 46 and updated by the

reproduction information managing means B45. A user area in the disk medium 6 is shown in Fig. 9. The user area is divided into k blocks comprising a first block (49), a second block (50), a third block (51) ... and a k-th block (52). In the first block, an EMI 53, reproduction information 54 and AV data 55 are stored in this order. The reproduction information has been non-reproduced when the reproduction flag is "play_flag = 0", and has been reproduced when "play_flag = 1". Since the EMI information, the reproduction information and the AV data are thus paired and stored in the identical area, it possible to process the three types of information simultaneously by a single access to the disk medium, thereby reducing overheads of access to the disk medium.

[0107]

In the second embodiment described above, it is configured to prohibit a user from directly changing the reproduction information via the digital I/F means 1 even when the reproduction information is not recorded in the system area (i.e., even when the reproduction information is recorded in the user area), unlike the case with the first embodiment, by mixing the AV data and the reproduction information by means of the reproduction information generating and EMI mixing means 46 and separating the AV data from the reproduction information by

means of the reproduction information and EMI separating means 47. Thus, illegal tampering of the reproduction information is prevented and reliability of the hard disk apparatus of the present embodiment is improved.

[0108]

In addition, the EMI information may be separately recorded in the system area in the second embodiment. In turn, the EMI information may solely be recorded in the user area in the first embodiment like the second embodiment, and the reproduction information may be recorded in the system area. In other words, recording method of the reproduction information and the EMI information may be any one of the methods described in the first embodiment or the second embodiment.

[0109]

Embodiment 3

A third embodiment will be described below.

[0110]

In the present embodiment, a hard disk apparatus is described by way of an example of a recording and reproducing apparatus that enables a viewer to view a program at an arbitrary time after the program has been broadcasted in the case where licensing information of AV data transmitted from a broadcasting station is "copy never" that represents a prohibition of copying.

[0111]

In the present embodiment, such hard disk apparatus is realized by making the AV data whose licensing information is "copy never" to be recordable and making the AV data to be reproduced only once by erasing the AV data during or after its reproduction.

[0112]

The configuration will be described below in terms of points that are different from the first embodiment.

[0113]

The configuration of the present embodiment is shown in Fig. 26. Following points are different from the configuration of Fig. 2 used in the first mode of the embodiment. Namely, the configuration does not include a reproduction information managing means A and an invalid data outputting means. Further, the selecting switch 19 is continuously connected to the encrypted data outputting side. The data block access means can input judgment results of the EMI judging means and can perform an access depending on the results.

[0114]

Operation of such embodiment will be described below.

[0115]

In the present embodiment, it is assumed that AV data sent from an STB is recorded and reproduced by a hard

disk apparatus in the same manner as the first embodiment. Descriptions of authentication and exchange of keys between the STB and the hard disk apparatus of the present embodiment are omitted since they are the same as the first embodiment.

[0116]

It is assumed that a record command is received in accordance with the command of the access method 2 via the digital I/F means 1. Succeeding process will be described with reference to the flowchart of Fig. 22. In the case where EMI of the AV data is not 00, the selecting switch is so switched that the AV data goes through the encrypting means 20. In the case where the EMI is 00, the selecting switch 24 is so switched that the AV data does not go through the encrypting means. The encrypting means 20 decrypts the AV data that are encrypted by using a key that is received thereby. The stream access means 16 instructs the data block access means 18 to record a block x. The data block access means 18 informs the EMI access means 11 of a block number (= x) that is currently accessed. The EMI access means 11 records the EMI information detected by the EMI detecting means 9 with relating the information to the informed block number. Note that, in the case where the EMI is 10 (copy one generation), the EMI is rewritten to be 01 (no more copy) when recording the EMI information

on the disk medium (S50).

[0117]

Then, the block number is incremented by one, i.e., the block number is set to be $x = x + 1$ (S51). Next, it is judged if another command is received from the digital I/F means 1 (S52). The process is brought to an end if another command is received. In the case where no command is received, the process after receiving the record command is repeated until another command is received. The above is the case of recording AV data on the disk medium 6.

[0118]

There will be described a case wherein a hard disk apparatus reproduces AV data. A case of reproducing the AV data on a TV monitor is considered. It is assumed that the AV data recorded in the hard disk is recorded from an STB. Descriptions of authentication and exchange of keys between the TV monitor and the hard disk apparatus of the present embodiment are omitted since they are the same as the first embodiment.

[0119]

Two types of operations may be performed depending on when the AV data is erased. A first case is a case wherein the AV data is erased at a time after finishing reproduction, and a second case is a case wherein the AV data is erased per block during its reproduction.

[0120]

All the blocks are initialized by using erase flag = "false" as a start (S53). The erase flag corresponds to each of the blocks on one-to-one basis, and it means that the block must be erased afterwards if the erase flag is "true".

[0122]

It is assumed that the hard disk apparatus receives a reproduction command in accordance with the command of the access method 2 from the digital I/F means 1. The stream access means 16 instructs the data block access means 18 to reproduce a block x. The data block access means 18 informs of the EMI access means 11 of a block number (= x) that is currently accessed. At the same time, the data block access means 18 reads out the AV data from the disk medium 6 via the LBA access means 3 (S54). The EMI access means 11 reads out EMI information corresponding to the informed block number from the disk medium 6. The read out EMI information is judged by the EMI judging means 12, and the judgment results are sent to the authenticating and encrypting means 13. In the case where the EMI is 00 in the EMI judgment results (S55), the selecting switch 25 is switched to the side that the AV data does not go through the encrypting means 23, so that the AV data is outputted without being encrypted (S57). In the case where

the EMI is not 00 (S55), the selecting switch 25 is switched to the side that the AV data goes through the encrypting means 23.

[0123]

In the case where the EMI is 11, the erase flag corresponding to the block number is rewritten to be "true". Next, in the case where the EMI is not 00, the selecting switch 19 is switched to the side of the authenticating and encrypting means 13, so that the AV data is encrypted by the encrypting means 23 to be outputted via the digital I/F means 1 (S57).

[0124]

Next, the block number is incremented by one, i.e., the block number is set to be $x = x + 1$ (S58). Then, it is judged if another command is received from the digital I/F means 1 (S59). The process is brought to an end if another command is received. When the reproduction process completes, AV data of the blocks containing the reproduced blocks from the initial value number to the last value number each having the erase flag of "true" are erased or link information of the block x to the recording position on the disk is erased (S60). In the case where no other command is received, the process after receiving the reproduction command is repeated until another command is received. The above is the case of reproducing the AV data

in accordance with the first case.

[0125]

The second case will be described below with reference to the flowchart of Fig. 23.

[0126]

It is assumed that the hard disk apparatus receives a reproduction command in accordance with the command of the access method 2 from the digital I/F means 1. The stream access means 16 instructs the data block access means 18 to reproduce a block x. The data block access means 18 informs the EMI access means 11 of a block number (= x) that is currently accessed. At the same time, the data block access means 18 reads out the AV data from the disk medium 6 via the LBA access means 3 (S54). The EMI access means 11 reads out EMI information corresponding to the informed block number from the disk medium 6. The read out EMI information is judged by the EMI judging means 12, and the judgment results are sent to the authenticating and encrypting means 13 as well as to the reproduction judging means 27.

[0127]

In the case where the EMI is 00 in the EMI judgment results (S66), the selecting switch 25 is switched to the side that the AV data does not go through the encrypting means 23, so that the AV data goes through the

authenticating and encrypting means 13 and then the digital I/F means 1 to be outputted without being encrypted (S57). In the case where the EMI is not 00 (S66), the selecting switch 25 is switched to the side that the AV data goes through the encrypting means 23. Then, the selecting switch 19 is switched to the side of the authenticating and encrypting means 13, so that the AV data read out by the data block access means 18 is encrypted by the encrypting means 23, and then outputted via the digital I/F means 1. In the case where the EMI of the block x is 11, the data block access means 18 erases the block x; writes in invalid data; or erases link information of the block x to the recording position on the disk (S67). Next, the block x is set to be $x + 1$ (S68), and the process is brought to an end if a command other than a reproduction command is received (S69). In the case where the command is not received, the process after receiving the reproduction command is repeated until the command is received.

[0128]

The above is the case where the AV data is reproduced in accordance with the second case.

[0129]

In the case where the EMI of the AV data recorded in the hard disk is 11 (copy never), it is possible to reproduce the AV data of "copy never" once by erasing the

data blocks of the AV data; writing invalid data in; or erasing the link information to a recording position on the disk.

[0130]

In addition, there is described the case wherein a command is executed by the stream access means in accordance with the access method 2 in the present embodiment; however, the execution of command is not limited thereto, and the command may be executed by the file access means 15 in accordance with the access method 3. In this case, the order of record and reproduction is not the order of block numbers, but the order of block numbers managed by the file management information. That is to say, if the block to be recorded and reproduced at x-th turn is set as $f(x)$, the block x in Figs. 22 and 23 is replaced by the block $f(x)$. Further, the block x can be erased by performing the erase on the file management.

[0131]

It is possible to realize the present embodiment if the EMI is recorded with being mixed with the AV data as in the second mode of the embodiment.

[0132]

Embodiment 4

A fourth embodiment will be described below.

[0133]

In the present embodiment, a VCR (video cassette recorder) is described by way of example for a recording and reproducing apparatus that enables a viewer to view a program at an arbitrary time after a time on which the program is broadcasted in the case where licensing information of AV data transmitted from a broadcasting station is "copy never" that represents a prohibition of copying.

[0134]

In the present embodiment, such hard disk apparatus is realized by making the AV data whose licensing information is "copy never" to be recordable and making the AV data to be reproduced only once by using a reproduction information managing means.

[0135]

A basic configuration of the VCR is shown in Fig. 12. The VCR comprises a digital I/F 1, a stream control means 90, a memory access means 56, a recording and reproducing means 57, a control means 58, a head 60, a memory 59 and a tape medium 61.

[0136]

The digital I/F means 1 is the same as that described in the first embodiment. The stream control means 90 will be described later in this specification in terms of points different from that described in the first

embodiment. The memory access means 56 is a means for recording and reproducing EMI information, reproduction information and the like with respect to the memory 5 provided in the tape medium 61. The recording and reproducing means 57 is a means for outputting digital AV data after processing a reproduction signal sent from the head 60 and sending a recording signal to the head 60 after processing AV data sent from the stream control means 90. The control means 58 performs running control of the tape medium 61, tracking of the head 60 and control of the recording and reproducing means 57. The head 60 records a signal on the tape medium 61 or reproduce a signal on the tape medium 61. The memory 59 is incorporated in the tape medium 61 and serves to record or reproduce the EMI information, the reproduction information and the like.

[0137]

As mentioned above, the stream control means 90 will be described in terms of the points different from that of the first embodiment. A command executing means 62 is a means for executing a command received from the digital I/F means 1. That is to say, the command executing means 61 understands the process contents of the command and instructs the control means 58 of reproduction, record, stop or the like. Such command to be sent to the I/F means 1 includes a method according to AV/C digital Interface

Command Set VCR subunit Specification version 2.0.1. In addition, the recording and reproducing means 57 is used in place of the data block access means 18 used in the first embodiment. The recording and reproducing means 57 is a means for informing the reproduction information managing means A of a track number that is currently recorded or reproduced.

[0138]

Operation of the present embodiment will be the same as that of the first embodiment if "block" in the first embodiment is replaced by "track" as well as the file access means 15 and the stream access means are replaced by the command executing means 62. Thus, there is realized the VCR that enables a viewer to view a program at an arbitrary time after a time on which the program is broadcasted in the case where licensing information of AV data transmitted from a broadcasting station is "copy never" that represents a prohibition of copying.

[0139]

Here, the following two cases will be described by way of example for storing the reproduction information and the AV data on the tape medium.

[0140]

A case wherein the reproduction information is retained by a track unit will be described first.

Referring to Fig. 14, the tape medium 61 is constituted by k tracks. A memory 59 is incorporated into the tape medium 61, and a reproduction information recording section 67 is recorded in the memory 59. Each of the reproduction information of a first track (63), a second track (64), a third track (65) and a k-th track (66) is represented by 0 in a table stored in the bit map form. That is to say, the areas are non-reproduced. Note that the area of the k-th track or the like is a free area, and such free area is represented by 0 in terms of the reproduction information. In turn, the reproduction information of an eleventh track, a twelfth track and a thirteenth track each is represented by 1, which means that the areas are used areas. The reproduction information recording section 67 is created and updated by the reproduction information managing means A17. Since the reproduction information recording section 67 is stored in the memory 59 incorporated by the tape medium 61, it is possible to prevent a user from tampering contents of the reproduction information recording section 67 easily to view the AV data illegally. Thus, reliability of the VCR of the present embodiment is improved.

[0141]

A case wherein the reproduction information is managed by using addresses will be described below. Referring to Fig. 15, a stream is defined by divining data

every time the reproduction information changes from reproduced to non-reproduced or from non-reproduced to reproduced in a whole tape portion 73 of the tape medium. The reproduction information recording section 67 is represented by reproduction information of the stream and a pair of a start track and an end track of the stream. A first stream (69) has the start track of 0 and the end track of a1, and all data of the stream are non-reproduced. A second stream (70) has the start track of a1 and the end track of a2, and all data of the stream are reproduced. A third stream (71) has the start track of a2 and the end track of a3, and all data of the stream are non-reproduced. An n-th stream (72) has the start track of a4 and the end track of a5, and reproduction information of the stream is reproduced. Such reproduction information recording section 67 is created and updated by the reproduction information managing means A17. Since the reproduction information recording section 67 is stored in the memory 59, it is possible to prevent a user from tampering contents of the reproduction information recording section 67 easily to view the AV data illegally. Thus, reliability of the VCR of the present embodiment is improved.

[0142]

Embodiment 5

A fifth embodiment will be described below.

[0143]

In the present embodiment, a VCR (video cassette recorder) is described by way of example for a recording and reproducing apparatus that enables a viewer to view a program at an arbitrary time after a time on which the program is broadcasted in the case where licensing information of AV data transmitted from a broadcasting station is "copy never" that represents a prohibition of copying. In the present embodiment, EMI information is paired with AV data to be recorded on a tape unlike the fourth embodiment. Further, such VCR is realized by making the AV data whose licensing information is "copy never" to be recordable and erasing the AV data with reproducing the same.

[0144]

Fig. 16 is a basic configuration of the VCR. As shown in Fig. 12, the points different from the VCR of the fourth embodiment are that the recording and reproducing means of the fourth embodiment is separated into a reproducing means and a recording means; the head is separated into a recording head and a reproducing head; and a separating means and a mixing means are newly provided in the present embodiment. The VCR comprises a digital I/F 1, a stream control means 91, a separating means 77, a reproducing means 78, a mixing means 79, a recording means

80, a control means 81, a head 74, a recording head, a reproducing head 76 and a tape medium.

[0145]

The digital I/F means 1 is the same as that described in the first embodiment. The stream control means 91 will be described later in this specification in terms of the points different from that of the fourth embodiment. The separating means 77 is a means for separating data read out from the reproducing means 78 into EMI information and AV data. The mixing means 79 is a means for pairing the EMI information and the AV data. The reproducing means 78 is a means for reproducing the EMI information and the AV data recorded on the tape medium 61 via the reproducing head 76 of the head 74. The recording means 80 is a means for recording the EMI information and the AV data on the tape medium via the recording head 75. The head 74 comprises the recording head 75 and the reproducing head 76 and is a means for reproducing a signal recorded on the tape medium 61 by using the reproducing head 76 as well as recording a signal on the tape medium 61 by using the recording head 75. The control means 81 is a means for performing a running control of the tape medium 61; a tracking of the head 74; and a control of the reproducing means 78 and the recording means 80. The tape medium 61 serves to record the signals.

[0146]

The points different from the stream control means 91 of the fourth embodiment mentioned above are as follow. A selecting switch 82 is so switched as to output outputted data from the authenticating and encrypting means 13 as they are during recording and is switched to the invalid data outputting means when judgment results of the EMI judging means 12 is EMI = 11 during reproduction. In the case of reproduction and EMI = 01 or 10, the selecting switch does not provide connection to the authenticating and encrypting means 13 nor the invalid data outputting means 14. The command executing means 62 is a means for informing the selecting switch 82 whether data are being recorded or reproduced in addition to contents described in the fourth embodiment. The reproduction information managing means A is not used in the present embodiment.

[0147]

The operation of the present embodiment will be described below.

[0148]

In the present embodiment, it is assumed that AV data sent from an STB are recorded and reproduced by a VCR in the same manner as the first embodiment. Descriptions of authentication and exchange of keys between the STB and the VCR of the present embodiment are omitted since they

are the same as the first embodiment.

[0149]

It is assumed that a record command is received by the command executing means 62 via the digital I/F means 1. The command executing means 62 informs the selecting switch 82 of the receipt of the record command. The selecting switch 82 is so switched that the AV data is sent from the authenticating and encrypting means 13 to the mixing means 79. In the case where the EMI of the AV data is not 00, the selecting switch is so switched that the AV data goes through the decrypting means 20. In the case where the EMI is 00, the selecting switch 24 is so switched that the AV data does not go through the decrypting means 20. The decrypting means 20 decrypts the encrypted AV data by using a key sent from the STB. The mixing means 79 receives EMI information that is detected by the EMI detecting means 9 and the AV data outputted by the authenticating and encrypting means 13 via the selecting switch 82. The mixing means 79 makes a pair of the EMI information and the AV data received thereby. Then, the recording means 80 records the pair of the AV data and the EMI information on the tape medium via the recording head 75 of the head 74. Note that, in the case where the EMI is 10 (copy one generation), the EMI is rewritten to be 01 (no more copy) and then the EMI information is recorded on the disk medium

6. A format in which the AV data and the EMI information are recorded on the tape medium 61 will be described later in this specification. The above process is continued until another command is received. The above is the process in the case of recording the AV data on the tape medium 61.

[0150]

A case wherein a VCR reproduces AV data will be described below. The description is focused on a case of reproducing the AV data on a TV monitor. It is assumed that the AV data recorded in the VCR is recorded from an STB. Descriptions of authentication and exchange of keys between the TV monitor and the VCR of the present embodiment are omitted since they are the same as those of the first embodiment.

[0151]

It is assumed that the VCR receives a reproduction command from the digital I/F means 1. The command executing means 62 informs the selecting switch 82 of the reception of the reproduction command. The selecting switch is switched to the side of the invalid data outputting means in the case where EMI in the judgment results of the EMI judging means 12 is 11. In the case where "EMI = 10" or "EMI = 01", the selecting switch 82 does not provide connection to the authenticating and

encrypting means 13 nor the invalid data outputting means 14. Note that AV data wherein "EMI = 10" does not exist in this case since the AV data treated in the present embodiment is recorded from the STB. That is to say, among EMI of the AV data, those of 10 are all rewritten to be "EMI = 01" when they are recorded from the STB. The separating means 77 separates the AV data that are reproduced via the tape medium 61, the head 74 and the reproducing means 78 from the EMI information. The AV data is sent to the authenticating and encrypting means 13. The EMI information is sent to the EMI applying means 10, and the AV data goes out of the authenticating and encrypting means 13 and then enters the EMI applying means 10. At the EMI applying means 10, the AV data is given the EMI and then outputted via the digital I/F means 1. Immediately after the separating means 77 separates the AV data from the EMI information, the mixing means 79 writes invalid data via the invalid data outputting means 14 on the tape medium 61 via the recording means 80 and the recording head 75 of the head 74 when the EMI is 11. The AV data on the tape medium 61 thus reproduced are replaced by the invalid data such as a blue back screen or a black screen. Thus, there is realized the VCR that enables a viewer to view a program at an arbitrary time after a time on which the program is broadcasted in the case where licensing

information of AV data transmitted from a broadcasting station is "copy never" that represents a prohibition of copying.

[0152]

As mentioned above, the format in which the AV data and the EMI information are recorded on the tape medium 61 will be described.

[0153]

As shown in Fig. 18, the tape 84 performs recording by the track unit, and the recorded track is given a track number 84. One track is divided into two areas; one is an EMI information recording section 85 and the other is a data recording section 86. The EMI information recording section 85 records EMI information. The data recording section 86 records AV data.

[0154]

In addition, the EMI information in the present invention is not limited to that recorded in the EMI information recording section in the above-described embodiment. A memory may be provided on the tape medium to record the EMI information in the memory. Such modification will make it hard to tamper information, thereby improving the reliability of the system.

[0155]

In the present embodiment, a hard disk apparatus

will be described by way of example for a recording and reproducing apparatus that enables a viewer to view a program at an arbitrary time after a time on which the program is broadcasted in the case where licensing information of AV data transmitted from a broadcasting station is "copy never" that represents a prohibition of copying. In the present embodiment, such hard disk apparatus is realized by making the AV data whose licensing information is "copy never" to be recordable; recording the AV data after re-encryption by using a second encrypting/decrypting means; and reproducing the AV data with erasing a key used by the second encrypting/decrypting means.

[0157]

Fig. 1 is a basic configuration of the hard disk apparatus of the present invention. This is the same as that described in the first embodiment. The stream control means 2 in the hard disk apparatus shown in Fig. 1 is configured as that shown in Fig. 19. That is to say, the stream control means 2 comprises an EMI detecting means 9, an EMI applying means 10, an EMI access means 11, an EMI judging means 12, an authenticating and encrypting means 13, an file access means 15, an stream access means 16, an data block access means 18, a time-variant key means 87, a key access means 88 and a second encrypting/decrypting means 89.

[0158]

Only the parts of the stream control means 2 different from that of the first embodiment will be described. The time-variant key means 87 is a means for generating a key that varies with time at random, and the generated key is a means that is sent to the key access means 88 as well as to the second encrypting/decrypting means 89. The key access means 88 is a means for recording the key generated by the time-variant key generating means 87 with relating it to a corresponding data block on the disk medium 6 and reading out the key from the disk medium 6. The second encrypting/decrypting means 89 is a means for encrypting or decrypting the AV data based on the key that is inputted thereto.

[0159]

Operation of the present embodiment will be described below.

[0160]

In the present embodiment, it is assumed that the hard disk apparatus records and reproduces AV data sent from an STB in the same manner as the first embodiment. Descriptions of authentication and exchange of keys between the STB and the hard disk apparatus of the present embodiment are omitted since they are the same as the first embodiment.

[0161]

It is assumed that a record command is received in accordance with the command of the access command 2 via the digital I/F means 1. Succeeding process will be described with reference to the flowchart of Fig. 20. In the case where EMI of the incoming AV data is not 00, the selecting switch 24 is so switched via the digital I/F means 1 so that the AV data goes through the decrypting means 20. In the case where the EMI is 00, connection is so provided that the AV data does not go through the decrypting means 20. The decrypting means 20 decrypts the encrypted AV data by using the key received thereby. The stream access means 16 instructs the data block access means 18 to record a block x. The data block access means 18 informs the EMI access means of a block number (= x) that is currently accessed. The EMI access means 11 records EMI information detected by the EMI detecting means 9 with relating the EMI information to the informed block number. Note that, if the EMI is 10 (copy one generation), the EMI is rewritten to 01 (no more copy) when the EMI information is recorded on the disk medium 6. The time-variant key means 87 generates a key. The generated key is sent to the key access means 88 and then recorded on the disk medium 6 via the LBA access means 3 (S26). The key is sent to the second encrypting/decrypting means 89, and the AV data sent

from the authenticating and encrypting means 13 are re-encrypted. The re-encrypted AV data is sent to the data block access means 18, and then recorded on the disk medium 6 via the LBA access means 3 (S27). Next, the block number is incremented by one, i.e., the block number is set to be $x = x + 1$ (S28). Then, it is judged if another command is received from the digital I/F means 1 (S29). If another command is received, the process is brought to an end. If not, the process after receiving the record command is repeated until another command is received. The above is the case of recording the AV data on the disk medium 6.

[0162]

A case wherein the hard disk apparatus reproduces AV data will be described below. A case of reproducing the AV data on the TV monitor is considered. It is assumed that the AV data recorded on the hard disk is recorded from an STB. Descriptions of authentication and exchange of key between the TV monitor and the hard disk apparatus of the present embodiment are omitted since they are the same as the first embodiment.

[0163]

Two types of reproduction operations can be performed depending on when the key generated by the time-variant key generating means 87 is erased from the disk medium 6. A first case is a case wherein the key is

deleted at a time after completing the reproduction, and a second case is a case wherein the key is erased per block during the reproduction.

[0164]

The first case will be described with reference to the flowchart of Fig. 20.

[0165]

It is assumed that the hard disk apparatus receives a reproduction command in accordance with the command of the access method 2 from the digital I/F means 1. The stream access means 16 instructs the data block access means 18 to reproduce a block x. The data block access means 18 informs the EMI access means 11 and the key access means 88 of a block number (= x) that is currently accessed. At the same time, the data block access means 18 reads out the AV data from the disk medium 6 via the LBA access means 3 (S30). The EMI access means 11 reads out EMI information corresponding to the informed block number from the disk medium 6. The read out EMI information is judged by the EMI judging means 12, and the judgment results are sent to the authenticating and encrypting means 13 as well as to the key access means 88. The key access means 88 reads out a key of the block x from the disk medium 6 (S1). The key access means 88 sends the read out key to the second encrypting/decrypting means 89, and the second

encrypting/decrypting means 89 decrypts the AV data of the block x sent from the data block access means 18 (32). The Key access means 88 set an erase flag of the key of the block x to 0 (S33). In the case where the EMI in the EMI judgment results is 00 (S34), the selecting switch 25 is switched to the side that the A data does not go through the encrypting means 23, so that the AV data is outputted without being encrypted. In the case where the EMI is not 00 (S34), the selecting switch 25 is switched to the side that the AV data goes through the encrypting means 23.

[0166]

In the case where the EMI is 11 (copy never), or in the case where the EMI is 01 (no more copy), the second encrypting/decrypting means 89 sends the decrypted AV data of the block x to the authenticating and encrypting means 13.

[0167]

After that, the key access means 88 sets the erase flag of the key of the block x to 1 (S35). Next, the block number is incremented by one, i.e., the block number is set to be $x = x + 1$ (S36). Then, it is judged if another command is received from the digital I/F means (S37). If another command is received, the process is brought to an end. When the reproduction process completes, the key access means erases a key or keys whose erase flag is/are 1

among those of blocks from initial value number to the last value number in the case where the EMI is 11 (S38). The erasing operation may be performed by substituting the recording portion of the key with invalid data or by erasing link information to the recording position on the disk medium whereon the key or keys is recorded.

[0168]

The second case will be described below with reference to the flowchart of Fig. 21.

[0169]

It is assumed that the hard disk receives a reproduction command in accordance with the command of the access method 2 from the digital I/F means 1. The stream access means 16 instructs the data block access means 18 to reproduce a block x. The data block access means 18 informs the EMI access means 11 and the key access means 88 of a block number (= x) that is currently accessed. At the same time, the data block access means 18 reads out the AV data from the disk medium 6 via the LBA access means 3 (S43). The EMI access means 11 reads out EMI information corresponding to the informed block number from the disk medium 6. The read out EMI information is judged by the EMI judging means 12, and the judgment results are sent to the authenticating and encrypting means 13 as well as to the key access means 88. The key access means 88 reads out

a key of the block x from the disk medium 6 (S44). The key access means 88 sends the read out key to the second encrypting/decrypting means 89, and the second encrypting/decrypting means 89 decrypts the AV data of the block x sent from the data block access means 18 (S45). In the case where the EMI in the EMI judgment results is 00 (S46), the selecting switch 25 is switched to the side that the AV data does not go through the encrypting means 23, so that the AV data is outputted without being encrypted. In the case where the EMI is not 00 (S46), the selecting switch 25 is switched to the side that the AV data goes through the encrypting means 23.

[0170]

In the case where the EMI is 11 (no more copy), the second encrypting/decrypting means 89 sends the decrypted AV data of the block x to the authenticating and encrypting means 13. After that, the key access means 88 erases the key of the block x (S47). The erasing operation may be performed by substituting the recording portion of the key with invalid data or by erasing link information to the recording position on the disk medium whereon the key is recorded.

[0171]

In the case where the EMI is 01 (no more copy), the second encrypting/decrypting means 89 outputs the decrypted

AV data of the block x . In this case, the key of the block x is not erased (S47).

[0172]

Next, the block number is incremented by one, i.e., the block number is set to be $x = x + 1$ (S48). Then, it is judged if another command is received from the digital I/F means 1 (S49). If another command is received, the process is brought to an end.

[0173]

Thus, since the AV data is recorded in the medium after being encrypted in the present embodiment, it is possible to enhance safety with respect to an illegal use compared with the case of recording the AV data without encrypting it in the case where exchangeable medium such as a DVD-RAM is used as the medium.

[0174]

In addition, the key recording method of the present embodiment may be modified to record a key with relating it to AV data. In this case, the key may be recorded in an area that a user cannot directly access such as a system area. Further, the area that the user cannot directly access is not limited to the system area, and the area may be an alternating sector area, a PVA, an RMA, a lead-in, a lead-out or a header section on a DVD-RAM medium as described in the first embodiment. That is to say, the

area may be any area as long as the user cannot access directly thereto. Thus, it is possible to prevent the user from accessing and reading the data of the key, thereby enhancing the safety.

[0175]

Further, although the method for reproducing the data once by deleting the key during reproduction is described in the present embodiment, it is possible to realize the same function by managing the reproduction information of the keys. That is to say, it is possible to reproduce the AV data encrypted and recorded on the recording medium once by managing the information indicating whether or not the key is read out as the reproduction information of the key in the same manner as the management of the reproduction information described in the first or the second embodiment so that the key is read out only once.

[0176]

Further, it is possible to increase the safety by recording the reproduction information of the key in an area that the user cannot access.

[0177]

Although the apparatus that can reproduce the AV data of "EMI = 11" (copy never) once is described in the first to sixth modes of embodiments, it is possible to

transfer the AV data among devices by reproducing the AV data as "EMI = 10" (copy one generation) only once in the case where the AV data of EMI = 10 (copy one generation) is recorded after being rewritten to be the AV data of "EMI = 01" (no more copy). In this case, it is possible to realize the transfer operation in the same manner as the first to sixth modes of embodiments except for outputting the AV data that is recorded as "EMI = 01" after rewriting it to be the AV data of "EMI = 10" with respect to a command requesting the transfer of the AV data. The transfer of AV data of EMI = 11 has already been described in the first embodiment, and it is possible to transfer the AV data other than that of "EMI = 11" as described above. Thus, this confers an advantage on the user to select a medium for storing the AV data freely.

[0178]

Although the EMI is used in the first to sixth modes of embodiments, it is possible to use CGMS to judge a presence or absence of license and a type of the license. In the case of using the CGMS for judging the presence or absence of license and the type of the license, a transport decoder may be required in the recording and reproducing apparatus of the present invention to complicate the configuration of the apparatus; however, the effect is the same as the case of using the EMI. If the CGMS is used,

the AV data that is copied once as "copy one generation" is outputted as it is (copy one generation) to be reproduced once.

[0179]

The invalid data of the present invention is not limited to the blue back screen and the black screen, and it is possible to use any data other than the AV data that is an object for reproduction such as a test pattern, a white screen and a screen wherein shown a message that says viewing of the data is not allowed.

[0180]

The time-variant key generating means of the present invention is not limited to the means for generating a key for each of blocks as that in the present embodiment, and it is possible to use any means as long as it generates a key that varies with time such as that generates a key for every 2 blocks or for every 4 blocks.

[0181]

The hard disk apparatus of the present embodiment is an example of the recording and reproducing apparatus of the present invention; the VCR of the present embodiment is an example of the recording and reproducing apparatus of the present invention; the reproduction information managing means, the EMI access means, the data block access means of the present embodiment are examples of the

recording means of the present invention; and the EMI access means, the reproduction information managing means, the data block access means and the selecting switch are examples of the reproducing means of the present invention.

[0182]

The recording and reproducing apparatus of the present invention is not limited to the hard disk apparatus and the VCR of the present embodiment, and it is possible to use any means as long as it can record and reproduce such as an optical disk apparatus and a DVD-RAM apparatus.

[0183]

The LBA access means described in the first to sixth modes of embodiments may be an access means based on a head, a cylinder and a sector in the case of using a hard disk apparatus. In the case of using an optical disk apparatus, there may be used an access means based on a minute, a second and a frame (one frame is 1/75 second). That is to say, any means may be used as long as it can realize a physical access to a disk medium.

[0184]

In the first to sixth modes of embodiment, it is possible to baffle the authentication with or to arrange not to send the key for decryption of AV data in place of outputting the invalid data to a device to which the AV data whose reproduction information is reproduced is

outputted.

[0185]

Further, a program recording medium characterized by storing a program for letting a computer to execute whole or a part of functions of the recording and reproducing apparatus of the present invention belongs to the present invention.

[0186]

[Effect of the Invention]

As is apparent from above descriptions, the present invention provides a recording and reproducing apparatus and a program recording medium that enable a viewer to view AV data, in the case where information representing licensing information of a program is a prohibition of copying, in accordance with the copyright holder's intention to permit one-time-only viewing and free from limitation on time after the AV data has been broadcasted. Also, the present invention provides a recording and reproducing apparatus that enables a user to select a medium for storage freely by making it possible to transfer AV data as a result of reproducing the AV data only for twice in the case where the licensing information represents a prohibition of copying or a permission of copying only for one generation.

[Brief Description of the Drawings]

[Fig. 1]

Fig. 1 is an illustration of a basic configuration of the hard disk apparatus according to the first, second, third and sixth modes of embodiments of the present invention.

[Fig. 2]

Fig. 2 is a block diagram showing a configuration of the stream control means in the case of recording the reproduction information and the data block separately in different areas according to the first embodiment of the present invention.

[Fig. 3]

Fig. 3 is a block diagram showing a configuration of the authenticating and encrypting means according to the first to sixth modes of embodiments of the present invention.

[Fig. 4]

Fig. 4 is a block diagram showing a configuration of the reproduction information managing means A according to the first and fourth modes of embodiments of the present invention.

[Fig. 5]

Fig. 5 is an illustration of the recording method for recording reproduction information by data block unit in a system area in the case of recording the reproduction

information and the data block separately in different areas on a disk medium according to the first embodiment of the present invention.

[Fig. 6]

Fig. 6 is an illustration of the recording method for recording reproduction information by using a start LBA and an end LBA with respect to which the reproduction information changes in the case of recording the reproduction information and the data block separately in different areas in a disk medium according to the first embodiment of the present invention.

[Fig. 7]

Fig. 7 is a block diagram showing a configuration of the stream control means in the case of recording reproduction information and a data block in an identical area according to the second embodiment of the present invention.

[Fig. 8]

Fig. 8 is a block diagram showing a configuration of the reproduction information managing means B in the case of recording reproduction information and a data block in an identical area on a disk medium according to the second embodiment of the present invention.

[Fig. 9]

Fig. 9 is an illustration of the recording method

for recording reproduction information and a data block in the case of recording the reproduction information and the data block in an identical area on a disk medium according to the second embodiment of the present invention.

[Fig. 10]

Fig. 10 are flowcharts showing a flow of process of recording AV data and a flow of process of reproducing AV data in accordance with the first and second modes of embodiments of the present invention; reproduction information is updated after completion of the reproduction in the flow of process of reproducing AV data.

[Fig. 11]

Fig. 11 are flowcharts showing a flow of process of recording AV data and a flow of process of reproducing AV data in accordance with the first and second modes of embodiments of the present invention; reproduction information is updated during the reproduction in the flow of process of reproducing AV data.

[Fig. 12]

Fig. 12 is an illustration of a basic configuration of the VCR according to the fourth embodiment of the present invention.

[Fig. 13]

Fig. 13 is a block diagram showing a configuration of the stream control means in the case of recording

reproduction information in a memory and recording AV data on a tape according to the fourth embodiment of the present invention.

[Fig. 14]

Fig. 14 is an illustration of the recording method for recording reproduction information by a track unit in the case of recording reproduction information in a memory and recording AV data on a tape according to the fourth embodiment of the present invention.

[Fig. 15]

Fig. 15 is an illustration of the recording method for recording reproduction information by using a start track and an end track with respect to which the reproduction information changes in the case of recording reproduction information in a memory and recording AV data on a tape according to the fourth embodiment of the present invention.

[Fig. 16]

Fig. 16 is an illustration of a basic configuration of the VCR according to the fifth embodiment of the present invention.

[Fig. 17]

Fig. 17 is a block diagram showing a configuration of the stream control means in the case of erasing AV data with reproducing it according to the fifth embodiment of

the present invention.

[Fig. 18]

Fig. 18 is an illustration of the recording method for recording EMI information and AV data on a tape in the case of erasing the AV data with reproducing it according to the fifth embodiment of the present invention.

[Fig. 19]

Fig. 19 is a block diagram showing a configuration of the stream control means in the case of recording AV data with re-encrypting it on a disk medium; decrypting the AV data when reproducing it to be outputted; and then erasing a key recorded on the disk medium according to the sixth embodiment of the present invention.

[Fig. 20]

Fig. 20 is a flowchart showing a flow of process in the case of erasing a key after reproducing AV data according to the sixth embodiment of the present invention.

[Fig. 21]

Fig. 21 is a flowchart showing a flow of process in the case of erasing a key during reproducing AV data according to the sixth embodiment of the present invention.

[Fig. 22]

Fig. 22 is a flowchart showing a flow of process in the case of erasing AV data after reproducing the AV data according to the third embodiment of the present invention.

[Fig. 23]

Fig. 23 is a flowchart showing a flow of process in the case of erasing AV data during reproducing it according to the third embodiment of the present invention.

[Fig. 24]

Fig. 24 is an illustration of the recording method of a DVD-R according to the first embodiment of the present invention.

[Fig. 25]

Fig. 25 is an illustration of the recording method of a DVD-RAM according to the first embodiment of the present invention.

[Fig. 26]

Fig. 26 is a block diagram showing a configuration of the stream control means in the case of erasing AV data during or after reproducing the AV data according to the third embodiment of the present invention.

[REFERENCE NUMERALS]

- 1 digital I/F means
- 2 stream control means
- 3 LBA access means
- 4 hard disk control means
- 5 actuator means
- 6 disk medium

- 7 head
- 8 spindle motor means
- 9 EMI detecting means
- 10 EMI applying means
- 11 EMI access means
- 12 EMI judging means
- 13 authenticating and encrypting means
- 14 invalid data outputting means
- 15 file access means
- 16 stream access means
- 17 reproduction information managing means A
- 18 data block access means
- 19 selecting switch
- 20 decrypting means
- 21 authenticating means
- 22 key generating means
- 23 encrypting means
- 24 selecting switch
- 25 selecting switch
- 26 reproduction information updating means
- 27 reproduction judging means
- 28 reproduction information generating means
- 29 reproduction information access means
- 30 selecting switch

FIG. 1

- 1 DIGITAL I/F MEANS
- 2 STREAM CONTROL MEANS
- 3 LBA ACCESS MEANS
- 4 HARD DISK CONTROL MEANS
- 5 ACTUATOR MEANS
- 6 DISK MEDIUM
- 7 HEAD
- 8 SPINDLE MOTOR MEANS

FIG. 2

- 1 I/F MEANS
- 2 STREAM CONTROL MEANS
- 3 LBA ACCESS MEANS
- 9 EMI DETECTING MEANS
- 10 EMI APPLYING MEANS
- 11 EMI ACCESS MEANS
- 12 EMI JUDGING MEANS
- 13 AUTHENTICATING AND ENCRYPTING MEANS
- 14 INVALID DATA OUTPUTTING MEANS
- 15 FILE ACCESS MEANS
- 16 STREAM ACCESS MEANS
- 17 REPRODUCTION INFORMATION MANAGING MEANS A
- 18 DATA BLOCK ACCESS MEANS
- 19 SELECTING SWITCH

51 DATA INPUT
52 AUTHENTICATING COMMAND
53 DATA OUTPUT
54 COMMAND IN ACCORDANCE WITH ACCESS METHOD 3
55 COMMAND IN ACCORDANCE WITH ACCESS METHOD 2
56 ENCRYPTED DATA INPUT
57 ENCRYPTED DATA OUTPUT
59 INFORM OF ACCESS POINT
60 DATA OUTPUT
61 EMI JUDGMENT RESULTS
62 DATA INPUT
63 BLOCK NUMBER
64 INFORM OF ACCESS POINT
65 BLOCK NUMBER
66 FILE MANAGEMENT INFORMATION
67 STREAM POINTER MANAGEMENT INFORMATION

FIG. 3

13 AUTHENTICATING AND ENCRYPTING MEANS
20 DECRYPTING MEANS
21 AUTHENTICATING MEANS
22 KEY GENERATING MEANS
23 ENCRYPTING MEANS
24 SELECTING SWITCH
51 ENCRYPTED DAT INPUT

52 AUTHENTICATING COMMAND
53 ENCRYPTING DATA OUTPUT
54 EMI JUDGMENT RESULTS
55 DATA INPUT
56 DATA OUTPUT

FIG. 4

3 LBA ACCESS MEANS
17 REPRODUCTION INFORMATION MANAGING MEANS A
18 DATA BLOCK ACCESS MEANS
19 SELECTING SWITCH
26 REPRODUCTION INFORMATION UPDATING MEANS
27 REPRODUCTION JUDGING MEANS
28 REPRODUCTION INFORMATION GENERATING MEANS
29 REPRODUCTION INFORMATION ACCESS MEANS
30 SELECTING SWITCH
51 INFORM OF WHICH BLOCK IS BEING ACCESSED

FIG. 5

32 USER AREA
33 REPRODUCTION INFORMATION RECORDING SECTION
34 FIRST BLOCK
35 SECOND BLOCK
36 THIRD BLOCK
37 k-TH BLOCK

51 BLOCKS

52 REPRODUCTION OF BLOCK k

FIG. 6

38 SYSTEM AREA

39 USER AREA

40 REPRODUCTION INFORMATION RECORDING SECTION

41 FIRST STREAM

42 SECOND STREAM

43 THIRD STREAM

44 n-TH STREAM

51 REPRODUCTION INFORMATION

52 START LBA

53 END LBA

FIG. 7

1 I/F MEANS

2 STREAM CONTROL MEANS

3 LBA ACCESS MEANS

9 EMI DETECTING MEANS

10 EMI APPLYING MEANS

12 EMI JUDGING MEANS

13 AUTHENTICATING AND ENCRYPTING MEANS

14 INVALID DATA OUTPUTTING MEANS

15 FILE ACCESS MEANS

16 STREAM ACCESS MEANS
17 REPRODUCTION INFORMATION MANAGING MEANS B
18 DATA BLOCK ACCESS MEANS
19 SELECTING SWITCH
46 REPRODUCTION INFORMATION GENERATING AND EMI MIXING MEANS
47 REPRODUCTION INFORMATION AND EMI SEPARATING MEANS
52 AUTHENTICATING COMMAND
54 COMMAND IN ACCORDANCE WITH ACCESS METHOD 3
55 COMMAND IN ACCORDANCE WITH ACCESS METHOD 2
56 ENCRYPTED DATA INPUT
57 ENCRYPTED DATA OUTPUT
58 REPRODUCTION JUDGMENT RESULTS
59 INFORM OF ACCESS POINT
60 DATA OUTPUT
61 EMI JUDGMENT RESULTS
62 DATA INPUT
63 BLOCK NUMBER
64 EMI INFORMATION
65 BLOCK NUMBER
66 FILE MANAGEMENT INFORMATION
67 STREAM POINTER MANAGEMENT INFORMATION
68 REPRODUCTION INFORMATION

FIG. 12

1 DIGITAL I/G MEANS

90 STREAM CONTROL MEANS
56 MEMORY ACCESS MEANS
57 RECORDING AND REPRODUCING MEANS
58 CONTROL MEANS
59 MEMORY
60 HEAD
61 TAPE MEDIUM

FIG. 8

3 LBA ACCESS MEANS
18 DATA BLOCK ACCESS MEANS
19 SELECTING SWITCH
26 REPRODUCTION INFORMATION UPDATING MEANS
27 REPRODUCTION JUDGING MEANS
29 REPRODUCTION INFORMATION ACCESS MEANS
45 REPRODUCTION INFORMATION MANAGING MEANS B
47 REPRODUCTION INFORMATION AND EMI SEPARATING MEANS
51 EMI JUDGMENT RESULTS
52 REPRODUCTION MANAGEMENT INFORMATION
53 INFORM OF WHICH BLOCK IS BEING ACCESSED

FIG. 9

53 EMI
54 REPRODUCTION INFORMATION
55 DATA

61 FIRST BLOCK
62 STRUCTURE OF DATA BLOCK
63 REPRODUCTION INFORMATION
play_flag
0 = non-reproduced
1 = reproduced
64 USER AREA

FIG. 16

1 DIGITAL I/F MEANS
91 STREAM CONTROL MEANS
77 SEPARATING MEANS
78 REPRODUCING MEANS
79 MIXING MEANS
80 RECORDING MEANS
81 CONTROL MEANS
74 HEAD
75 RECORDING HEAD
76 REPRODUCING HEAD
61 TAPE MEDIUM
ENLARGED VIEW OF HEAD

FIG. 10

51 AT THE TIME OF RECORDING
52 START

53 x = INITIAL VALUE
S1 play_flag = 0
S2 RECORD BLOCK x
S3 x = x + 1
S4 RECORDING FINISHED?
57 END
54 AT THE TIME OF REPRODUCTION
55 START
56 x = INITIAL VALUE
S5 LEAD BLOCK x
S6 EMI = 11
S7 play_flag
S8 OUTPUT BLOCK x
S9 x = x + 1
S10 OUTPUT DUMMY BLOCK OR STOP OUTPUTTING
S11 REPRODUCTION FINISHED?
S12 BLOCK x = INITIAL VALUE TO CURRENT VALUE ARE UPDATED BY
play_flag = 1
58 END

FIG. 11

51 AT THE TIME OF RECORDING
52 START
53 x = INITIAL VALUE
S13 play_flag = 0

S14 RECORD BLOCK x
S15 $x = x + 1$
S16 RECORDING FINISHED?
57 END
54 AT THE TIME OF REPRODUCTION
55 START
56 $x = \text{INITIAL VALUE}$
S17 LEAD BLOCK x
S18 $\text{EMI} = 11$
S19 play_flag
S20 $\text{play_flag} = 1$
S21 OUTPUT BLOCK x
S22 OUTPUT DUMMY BLOCK OR STOP OUTPUTTING
S23 RECORD (UPDATE) play_flag OF BLOCK x
S24 $x = x + 1$
S25 REPRODUCTION FINISHED?
58 END

FIG. 13

1 I/F MEANS
9 EMI DETECTING MEANS
10 EMI APPLYING MEANS
11 EMI ACCESS MEANS
12 EMI JUDGING MEANS
13 AUTHENTICATING AND ENCRYPTING MEANS

14 INVALID DATA OUTPUTTING MEANS

90 STREAM ACCESS MEANS

17 REPRODUCTION INFORMATION MANAGING MEANS A

19 SELECTING SWITCH

56 MEMORY SECTION ACCESS MEANS

57 RECORDING AND REPRODUCING MEANS

58 CONTROL MEANS

62 COMMAND EXECUTING MEANS

71 DATA INPUT

72 AUTHENTICATING COMMAND

73 DATA OUTPUT

74 ENCRYPTED DATA INPUT

75 ENCRYPTED DATA OUTPUT

76 COMMAND INPUT AND OUTPUT

77 DATA OUTPUT

78 EMI JUDGMENT RESULTS

79 DATA INPUT

80 INFORM OF TRACK NUMBER

81 INFORM OF TRACK NUMBER

FIG. 14

51 REPRODUCTION INFORMATION OF k-TH TRACK

59 MEMORY

67 REPRODUCTION INFORMATION RECORDING SECTION

63 FIRST TRACK

64 SECOND TRACK

65 THIRD TRACK

66 k-TH TRACK

68 WHOLE TAPE

FIG. 15

51 REPRODUCTION INFORMATION

52 START TRACK

53 END TRACK

59 MEMORY

67 REPRODUCTION INFORMATION RECORDING SECTION

69 FIRST STREAM

70 SECOND STREAM

71 THIRD STREAM

72 n-TH STREAM

73 WHOLE TAPE

FIG. 24

51 WHOLE DISK

52 DATA AREA

FIG. 17

1 I/F MEANS

9 EMI DETECTING MEANS

10 EMI APPLYING MEANS

12 EMI JUDGING MEANS

13 AUTHENTICATING AND ENCRYPTING MEANS

14 INVALID DATA OUTPUTTING MEANS
91 STREAM CONTROL MEANS
79 MIXING MEANS
77 SEPARATING MEANS
81 CONTROL MEANS
62 COMMAND EXECUTING MEANS
51 AUTHENTICATING COMMAND
52 COMMAND INPUT AND OUTPUT
53 ENCRYPTED DATA INPUT
54 ENCRYPTED DATA OUTPUT
55 DATA OUTPUT
56 EMI JUDGMENT RESULTS
57 DATA INPUT
58 DATA
59 DATA
60 EMI INFORMATION
61 EMI INFORMATION
63 EMI INFORMATION
64 INFORM OF RECORDING OR REPRODUCTION

FIG. 18

83 TRACK NUMBER
84 TAPE
85 EMI INFORMATION RECORDING SECTION
86 DATA RECORDING SECTION

FIG. 25

51 WHOLE DISK
52 FIRST ZONE
53 SECOND ZONE
54 n-TH ZONE
55 SECTOR
56 SECTOR
57 SECTOR
58 HEADER
59 DATA
60 ONE ZONE

FIG. 19

1 I/F MEANS
2 STREAM CONTROL MEANS
3 LBA ACCESS MEANS
9 EMI DETECTING MEANS
10 EMI APPLYING MEANS
11 EMI ACCESS MEANS
12 EMI JUDGING MEANS
13 AUTHENTICATING AND ENCRYPTING MEANS
15 FILE ACCESS MEANS
16 STREAM ACCESS MEANS
18 DATA BLOCK ACCESS MEANS

51 DATA INPUT
52 AUTHENTICATING COMMAND
53 DATA OUTPUT
54 COMMAND IN ACCORDANCE WITH ACCESS METHOD 3
55 COMMAND IN ACCORDANCE WITH ACCESS METHOD 2
56 ENCRYPTED DATA INPUT
57 ENCRYPTED DATA OUTPUT
59 INFORM OF ACCESS POINT
60 DATA OUTPUT
61 EMI JUDGMENT RESULTS
62 DATA INPUT
63 BLOCK NUMBER
64 BLOCK NUMBER
65 KEY IS RECORDED
66 FILE MANAGEMENT INFORMATION
67 STREAM POINTER MANAGEMENT INFORMATION
68 KEY
87 TIME-VARIANT KEY MEANS
88 KEY ACCESS MEANS
89 SECOND ENCRYPTING/DECRYPTING MEANS

FIG. 20

51 AT THE TIME OF RECORDING
52 START
53 x = INITIAL VALUE

S26 RECORD KEY OF BLOCK x
S27 RECORD BLOCK x AFTER DECRYPTION
S28 $x = x + 1$
S29 RECORDING IS FINISHED?
54 END
55 START
56 $x = \text{INITIAL VALUE}$
S30 LEAD BLOCK x
S31 READ OUT KEY OF BLOCK x AND ACCESS
S32 DECRYPT BLOCK x AND OUTPUT
S33 CLEAR ERASE FLAG OF KEY OF BLOCK x
S34 $\text{EMI} = 11$
S35 SET ERASE FLAG OF BLOCK x
S36 $x = x + 1$
S37 REPRODUCTION IS FINISHED?
S38 ERASE BLOCK OR BLOCKS AMONG BLOCK $x = \text{INITIAL VALUE TO}$
CURRENT VALUE WHOSE KEY HAS ERASE FLAG = 1
57 END

FIG. 21

51 AT THE TIME OF RECORDING
52 START
53 $x = \text{INITIAL VALUE}$
S39 RECORD KEY OF BLOCK x
S40 RECORD BLOCK x AFTER DECRYPTION

S41 $x = X + 1$
S42 RECORDING IS FINISHED?
54 END
55 START
56 $x = \text{INITIAL VALUE}$
S43 LEAD BLOCK x
S44 READ OUT KEY OF BLOCK x AND ACCESS
S45 DECRYPT BLOCK x AND OUTPUT
S46 $\text{EMI} = 11$
S47 ERASE KEY OF BLOCK x
S48 $x = x + 1$
S49 REPRODUCTION IS FINISHED?
57 END

FIG. 22

51 AT THE TIME OF RECORDING
52 START
53 $x = \text{INITIAL VALUE}$
S50 RECORD BLOCK x
S51 $x = x + 1$
S52 RECORDING IS FINISHED?
54 END
58 AT THE TIME OF REPRODUCTION
55 START
56 $x = \text{INITIAL VALUE}$

S53 INITIALIZE ALL BLOCKS BY ERASE FLAG = "FALSE"
S54 LEAD BLOCK x
S55 EMI = 11
S56 SET ERASE FLAG OF BLOCK = "TRUE"
S57 OUTPUT BLOCK x
S58 $x = x + 1$
S59 REPRODUCTION IS FINISHED?
S60 ERASE BLOCK OR BLOCKS AMONG BLOCK x = INITIAL VALUE TO
CURRENT VALUE WHOSE ERASE FLAG = TRUE
57 END

FIG. 23

51 AT THE TIME OF RECORDING
52 START
53 $x = \text{INITIAL VALUE}$
S61 RECORD BLOCK x
S62 $x = x + 1$
S63 RECORDING IS FINISHED?
54 END
58 AT THE TIME OF REPRODUCTION
55 START
56 $x = \text{INITIAL VALUE}$
S64 LEAD BLOCK x
S65 OUTPUT BLOCK x
S66 EMI = 11

S67 ERASE BLOCK x
S68 $x = x + 1$
S69 REPRODUCTION IS FINISHED?
57 END

FIG. 26

1 I/F MEANS
2 STREAM CONTROL MEANS
3 LBA ACCESS MEANS
9 EMI DETECTING MEANS
10 EMI APPLYING MEANS
11 EMI ACCESS MEANS
12 EMI JUDGING MEANS
13 AUTHENTICATING AND ENCRYPTING MEANS
15 FILE ACCESS MEANS
16 STREAM ACCESS MEANS
18 DATA BLOCK ACCESS MEANS
51 DATA INPUT
52 AUTHENTICATING COMMAND
53 DATA OUTPUT
54 COMMAND IN ACCORDANCE WITH ACCESS METHOD 3
55 COMMAND IN ACCORDANCE WITH ACCESS METHOD 2
56 ENCRYPTED DATA INPUT
57 ENCRYPTED DATA OUTPUT
59 INFORM OF ACCESS POINT

-128-

60 DATA OUTPUT

61 EMI JUDGMENT RESULTS

62 DATA INPUT

63 BLOCK NUMBER

65 BLOCK NUMBER

66 FILE MANAGEMENT INFORMATION

67 STREAM POINTER MANAGEMENT INFORMATION

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.